BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Galih (2012) dalam penelitiannya menyebutkan Penggunaan *Firewall* Mikrotik Sebagai Sistem Keamanan dan Manajemen *Bandwidth* Jaringan Komputer di PT. Astra Honda Motor Semarang digunakan untuk memenuhi kebutuhan sistem khususnya dalam pada sisi keamanan dan pembagian *bandwidth*. *Firewall* dan manajemen *bandwidth* di mikrotik digunakan untuk mengatasi *client* yang mendowload secara besar-besaran dan mengatur pembagian bandwidth. Implementasi aplikasi *firewall* begitu penting dimanfaatkan untuk mengatasi dampak dari setiap aktivitas download yang dilakukan oleh *client*.

Darno (2016) pada penelitian Tugas Akhir tentang Peningkatan Keamanan Jaringan Berbasis *Intrusion Detection System (IDS)* pada studi kasus Universitas Sahid Surakarta, membahas tentang penanganan *attacker* dengan sistem *IDS* sehingga pemanfaatan jaringan lebih stabil. Sistem monitor yang digunakan adalah *IDS*, tentunya hal ini menambah aplikasi tambahan, sementara di mikrotik sendiri memiliki *tools* untuk melakukan monitor jaringan.

Implementasi Manajemen *Bandwidth* dengan *Simple Queue* dan *Queue Tree* untuk mengetahui kelemahan dan kelebihan sistem jaringan, Amri (2016), tidak terlepas dari tantangan kebutuhan sistem keamanan jaringan dengan memanfaatkan mikrotik.

Keberadaan sistem keamanan jaringan dalam setiap pengelolaan jaringan menjadi sangat dibutuhkan. Berbagai penelitian di atas membuktikan pentingnya sistem keamanan jaringan, untuk itu diperlukan penelitian untuk mengimplementasikan sistem keamanan jaringan pada sebuah perangkat yang disebut Routherboard Mikrotik Haplite RB-951Ui-2HnD. Perangkat ini

memiliki fasilitas untuk keamanan jaringan dan pembatasan akses jaringan yaitu *packet filtering firewall*, fasilitas ini dapat digunakan untuk penanganan keamanan jaringan akibat penggunaan akses internet yang tidak semestinya dan tindakan pencegahan adanya serangan pada jaringan *hotspot*.

2.2. Teori – Teori Pendukung

2.2.1. Pengertian 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.* Menurut Andi Novianto (2012:7) pada model komputer yang bekerja sendiri tanpa terhubung dengan komputer lain disebut *stand alone* (masing-masing berdiri sendiri) sedangkan komputer yang semula bekerja sendiri kemudian terhubung melalui media transmisi dengan komputer lainnya untuk berkomunikasi disebut sebagai *network* (jaringan). Agar dapat saling berkomunikasi satu dengan lainnya masing-masing PC yang terkomunikasi dalam jaringan harus mengikuti aturan (protokol) yang sudah ditentukan atau disepakati bersama. Dengan protokol atau aturan yang sudah baku maka PC dengan sistem operasi dan *platform* yang berbeda dapat saling berkomunikasi. Dalam jaringan komputer sekarang ini *protocol* yang lazim dipakai adalah TCP/IP (*Transmission Control Protocol/Internet Protocol*). Selain *protocol* tersebut masih ada *protocol* OSI (*Open System Interconnection*).

Salah satu contoh penerapan protokol TCP/IP adalah bahwa setiap komputer yang terhubung ke jaringan harus memiliki alamat yang berbeda. Demikian juga dengan PC, setiap PC agar dapat saling bertukar *resource* harus dapat mengenali alamat masing-masing. Karena itu setiap PC yang terkoneksi ke jaringan diberi alamat tertentu, dalam TCP/IP dalam *format* angka 32 bit. Dalam berbagi *resource* maka salah satu PC berfungsi sebagai penyedia *resource* (*server*) sedangkan PC lain bertindak sebagai pengguna/pengakses *resource (client).* Dalam implementasinya menurut Iwan Sofana (2012:110) layanan yang

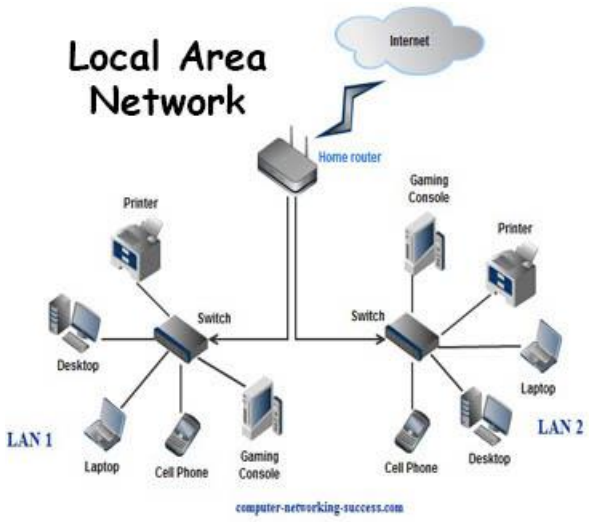
diberikan bisa berupa akses web, email, file atau yang lainnya. *Client* server banyak dipakai oleh internet dan intranet.

2.2.2. Jenis-Jenis Jaringan Komputer

2.2.2.1.Local Area Network

Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer dengan tujuan memakai bersama sumber daya dan saling bertukar informasi seperti yang ditunjukkan pada Gambar 2.1. *LAN* diciptakan untuk menghemat biaya dalam penggunaan alat secara bersama-sama, tetapi lama kelamaan fungsinya makin bertambah. Sebuah saluran komunikasi dapat digunakan secara bersama oleh banyak komputer yang terhubung satu dengan yang lain. Menurut Iwan Sofana, (2010:107) suatu himpunan interkoneksi sejumlah komputer *autonomous* atau kumpulan beberapa komputer dan perangkat lain seperti *router*, *switch* dan sebagainya yang saling terhubung satu sama lain melalui media perantara.

Berdasarkan jenis jaringannya, teknologi *LAN* dapat dibedakan menjadi tiga karakteristik yakni: ukuran, teknologi transmisi, dan topologinya. *LAN* mempunyai ukuran yang terbatas, yang berarti waktu transmisi dalam keadaan terburuknya terbatas dan dapat diketahui sebelumnya. *LAN* seringkali menggunakan teknologi transmisi kabel. *LAN* tradisional beroperasi pada kecepatan 10 sampai dengan 100 Mbps dan mempunyai faktor kesalahan yang kecil. *LAN* dapat dikembangkan dengan mudah dan mendukung kecepatan transfer data yang cukup tinggi (Iwan Sofana, 2010:113).



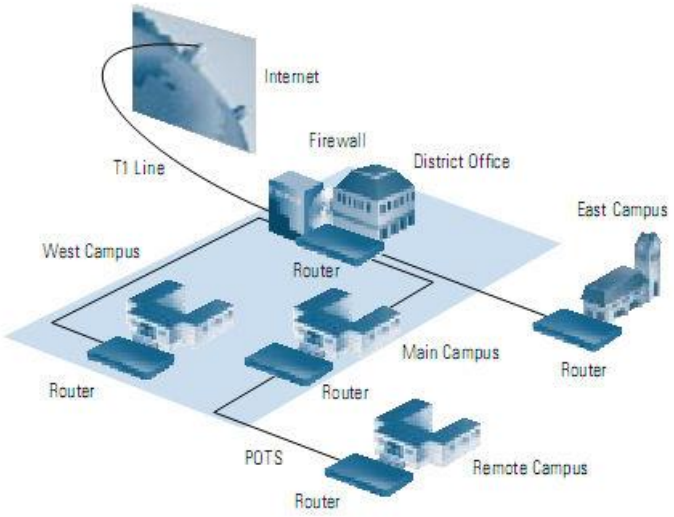
Gambar 2.1 Jaringan *LAN*

Beberapa model konfigurasi *LAN*, satu komputer biasanya dijadikan sebuah *file server*. Yang mana digunakan untuk menyimpan perangkat lunak (*software*) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung ke dalam *network*.

Komputer-komputer yang terhubung ke dalam jaringan (*network*) itu biasanya disebut dengan *workstation.* Biasanya kemampuan *workstation* lebih di bawah dari *file server* dan mempunyai aplikasi lain di dalam hardisknya selain aplikasi untuk jaringan. Kebanyakan *LAN* menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya.

2.2.2.2. *Metropolitan Area Network (MAN)* / Jaringan area Metropolitan

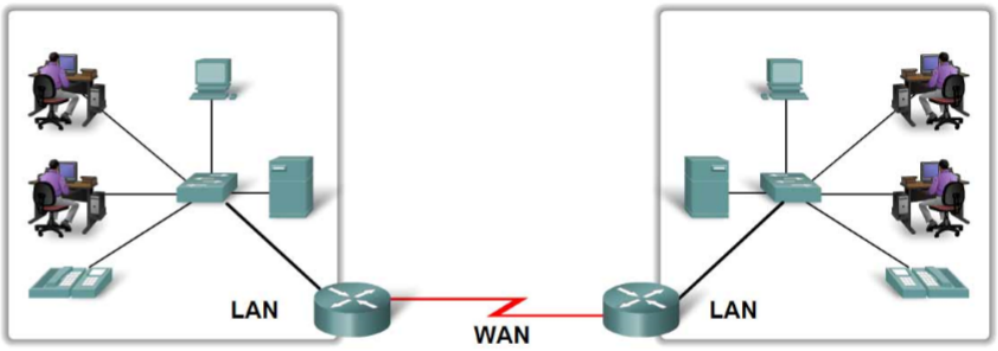
Jaringan *MAN* yang ditunjukkan pada Gambar 2.2. biasanya meliputi area yang lebih besar dari *LAN*. Sistem MAN sering dipergunakan untuk sambungan jarak jauh antarkantor atau organisasi yang masih dalam satu manajemen yang bertujuan untuk sinkronisasi sistem informasi, pengontrolan dan sentralisasi sistem (Novianto, 2012:10).



Gambar 2.2. Jaringan *MAN*

2.2.2.3. *Wide Area Network (WAN)* / Jaringan area Skala Besar

Wide Area Networks (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana satelit, *wireless*, ataupun kabel *fiber optic* karena jangkauannya yang lebih luas hingga otoritas negara lain. sebagai contoh jaringan telepon antar Negara seperti ditunjukkan pada Gambar 2.3.



Gambar 2.3 Jaringan *WAN*

Menggunakan sarana *WAN* biasanya agak rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara *LAN* dan *WAN* ke dalam Komunikasi Global seperti *Internet*. Tapi bagaimanapun juga antara *LAN*,

MAN dan *WAN* tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

2.3. Topologi Jaringan

Topologi Jaringan adalah hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node, link*, dan *station.* Dalam penyusunan topologi jaringan ini ada 6 macam topologi jaringan komputer, yaitu :

2.3.1. Topologi *Point to Point* (Titik ke-Titik).

Jaringan kerja titik ke titik merupakan jaringan kerja yang paling sederhana tetapi dapat digunakan secara luas. Begitu sederhananya jaringan ini, sehingga seringkali tidak dianggap sebagai suatu jaringan tetapi hanya merupakan komunikasi biasa. Dalam hal ini, kedua simpul mempunyai kedudukan yang setingkat, sehingga simpul manapun dapat memulai dan mengendalikan hubungan dalam jaringan tersebut. Data dikirim dari satu simpul langsung kesimpul lainnya sebagai penerima, misalnya antara terminal dengan CPU.

2.3.2. Topologi Bintang

Dalam konfigurasi bintang, beberapa peralatan yang ada akan dihubungkan kedalam satu pusat komputer. Kontrol yang ada akan dipusatkan pada satu titik, seperti misalnya mengatur beban kerja serta pengaturan sumber daya yang ada. Pada topologi star tidak langsung terhubung satu sama lain, tetapi melalui perangkat pusat pengendali (*central controller*) yang biasa disebut dengan HUB (Supriyanto:2013). Semua link harus berhubungan dengan pusat apabila ingin menyalurkan data ke simpul lainnya yang dituju. Dalam hal ini, bila pusat mengalami gangguan, maka semua terminal juga akan terganggu. Model jaringan bintang ini relatif sangat sederhana, sehingga banyak digunakan oleh instansi yang biasanya mempunyai banyak kantor cabang yang tersebar dipelbagai lokasi. Dengan adanya konfigurasi bintang ini, maka segala macam

kegiatan yang ada di kantor cabang dapatlah dikontrol dan dikoordinasikan dengan baik.

2.3.3. Topologi Cincin

Pada jaringan ini terdapat beberapa peralatan saling dihubungkan satu dengan lainnya dan pada akhirnya akan membentuk bagan seperti halnya sebuah cincin. Jaringan cincin tidak memiliki suatu titik yang bertindak sebagai pusat ataupun pengatur lalu lintas data, semua simpul mempunyai tingkatan yang sama. Data yang dikirim akan berjalan melewati beberapa simpul sehingga sampai pada simpul yang dituju. Dalam menyampaikan data, jaringan bisa bergerak dalam satu ataupun dua arah. Walaupun demikian, data yang ada tetap bergerak satu arah dalam satu saat. Pertama, pesan yang ada akan disampaikan dari titik ketitik lainnya dalam satu arah. Apabila ditemui kegagalan, misalnya terdapat kerusakan pada peralatan yang ada, maka data yang ada akan dikirim dengan cara kedua, yaitu pesan kemudian ditransmisikan dalam arah yang berlawanan, dan pada akhirnya bisa berakhir pada tempat yang dituju. Konfigurasi semacam ini relative lebih mahal apabila dibanding dengan konfigurasi jaringan bintang. Hal ini disebabkan, setiap simpul yang ada akan bertindak sebagai komputer yang akan mengatasi setiap aplikasi yang dihadapinya, serta harus mampu membagi sumber daya yang dimilikinya pada jaringan yang ada. Permasalahannya adalah sinyal akan semakin melemah apabila jarak yang harus ditempuh untuk mencapai tujuan semakin jauh. Karenanya untuk mengatasi lemahnya sinyal data karena kemungkinan menempuh jarak di luar batasan yang dibolehkan, maka setiap perangkat pada topologi ini dilengkapi dengan sebuah repeater (Supriyanto 2013:54).

2.3.4. Topologi Pohon / *Topology Tree*

Pada jaringan pohon atau *topology tree* ini mempunyai susunan jaringan yang bisa dibilang hampir mirip dengan pohon yang bercabang.Topologi ini juga sebenarnya “versi luas” topologi star.Pada topologi ini setiap node memiliki tingkat masing – masing.Node yang memiliki tingkat tinggi diletakkan di atas sedangkan untuk yang memiliki tingkat rendah diletakkan di bawah.Dalam

topologi ini sebuah node bisa mempunyai cabang layaknya pohon yang memiliki cabang yang mempunyai cabang lagi. Data yang dikirim oleh node tertentu harus melewati node pusat (node pusat cabang) untuk sampai pada tujuan. Jadi pada suatu kesempatan, jika node pusat tersebut rusak, maka node tertentu akan kesulitan untuk mengirim data ke node yang letaknya lebih jauh (Supriyanto, 2013:58)

Keunggulan jaringan model pohon seperti ini adalah, dapat terbentuknya suatu kelompok yang dibutuhkan pada setiap saat. Sebagai contoh, perusahaan dapat membentuk kelompok yang terdiri atas terminal pembukuan, serta pada kelompok lain dibentuk untuk terminal penjualan. Adapun kelemahannya adalah, apabila simpul yang lebih tinggi kemudian tidak berfungsi, maka kelompok lainnya yang berada dibawahnya akhirnya juga menjadi tidak efektif. Cara kerja jaringan pohon ini relatif menjadi lambat.

2.3.5. Topologi Bus

Dikenal dengan istilah *bus-network*, yang cocok digunakan untuk daerah yang tidak terlalu luas. Setiap komputer (setiap simpul) akan dihubungkan dengan sebuah kabel komunikasi melalui sebuah *interface*. Instalasi jaringan Bus sangat sederhana, murah & maksimal terdiri atas 5-7 komputer. Kesulitan yg sering dihadapi adl kemungkinan terjadinya tabrakan data karena mekanisme jaringan relatif sederhana & jika salah satu node putus maka akan mengganggu kinerja & trafik seluruh jaringan (Supriyanto, 2013:52)

2.3.6. Topologi Kombinasi / *Plex Network*

Merupakan jaringan yang benar-benar interaktif, dimana setiap simpul mempunyai kemampuan untuk meng-*access* secara langsung tidak hanya terhadap komputer, tetapi juga dengan peralatan ataupun simpul yang lain. Secara umum, jaringan ini mempunyai bentuk mirip dengan jaringan bintang. Organisasi data yang ada menggunakan desentralisasi, sedang untuk melakukan perawatan, digunakan fasilitas sentralisasi.

2.4. Protokol

2.4.1. Pengertian Protokol

Menurut Andi Novianto(2012:67), protokol adalah sebuah aturan baku yang bersifat standar mengenai prosedur terjadinya komunikasi data dalam jaringan. Aturan-aturan ini meliputi tata cara bagaimana agar computer bias saling berkomunikasi, biasanya berupa bentuk (model) komunikasi, waktu (saat berkomunikasi), barisan (*traffic* saat berkomunikasi, pemeriksaan *error* saat transmisi data dan lain-lain. Faktor-faktor yang harus diperhatikan dalam protokol adalah : *sintaksis, semantic* dan *timing.* Secara rinci fungsi protocol adalah sebagai berikut :

a. Fragmentasi dan perakitan ulang *(reassembly)*
b. Enkapsulasi *(encapsulation)*
c. Kontrol koneksi *(connection control)*
d. Kontrol aliran *(flow control)*
e. Kontrol kesalahan *(error control)*
f. Layanan transmisi *(transmision service)*

2.4.2. Pengertian Model Osi Layer

Pengertian model ***OSI*** *(Open System Interconnection)* adalah suatu model konseptual yang terdiri atas tujuh layer, yang masing-masing layer tersebut mempunyai fungsi yang berbeda. *OSI* dikembangkan oleh badan Internasional yaitu *ISO (International Organization for Standardization)* pada tahun 1977. Model ini juga dikenal dengan model tujuh lapis *OSI (OSI seven layer model)* seperti ditunjukkan pada Tabel 2.1.

Tabel 2.1 Tabel Model *OSI Layer*

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Definisi masing-masing *Layer* pada model *OSI*

1) *Application* adalah *layer* paling tinggi dari model *OSI*, seluruh *layer* dibawahnya bekerja untuk *layer* ini, tugas dari *application layer* adalah Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, NFS.
2) *Presentation* berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam windows NT) dan

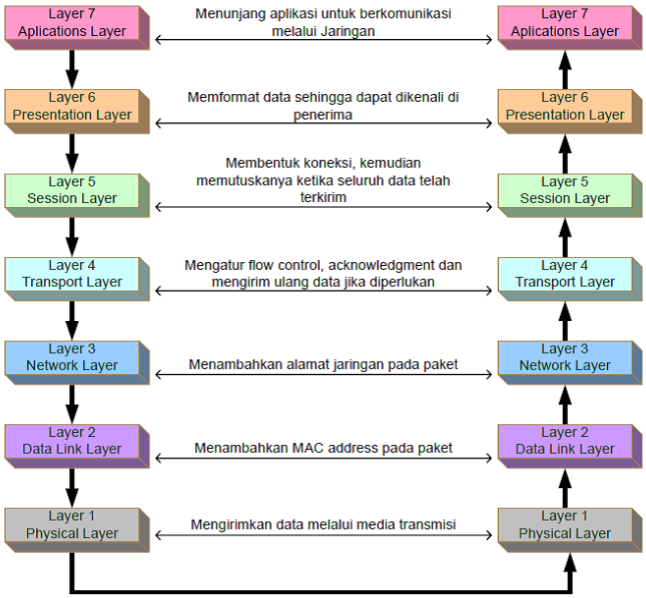
juga *Network shell* (semacam *Virtual Network Computing (VNC)* atau *Remote Dekstop Protokol (RDP).*

3) *Session* berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4) *Transport* berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses *(acknowledgement),* dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
5) *Network* berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing melalui *internetworking* dengan menggunakan *router* dan *switch* layer3.
6) *Data Link* berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras seperti halnya Media Access Control Address (MAC Address), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch* beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Access Control (MAC*).
7) *Physical* adalah *layer* paling bawah dalam model *OSI*. Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card (NIC)* dapat berinteraksi dengan media kabel atau radio.

2.4.3. Cara Kerja Model OSI

Pembentukan paket dimulai dari layer teratas model *OSI* ditunjukkan pada Gambar 2.4. *Application layer* megirimkan data ke *presentation layer*, di *presentation layer* data ditambahkan *header* dan atau *tailer* kemudian dikirim ke

layer di bawahnya, pada *layer* di bawahnya pun demikian, data ditambahkan *header* dan atau *tailer* kemudian dikirimkan ke *layer* dibawahnya lagi, terus demikian sampai ke *physical layer*.



Gambar 2.4 Cara Kerja Model *OSI*

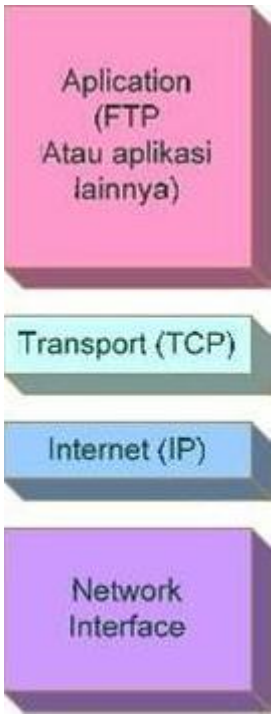
Di *physical layer* data dikirimkan melalui media transmisi ke *host* tujuan. Di *host* tujuan paket data mengalir dengan arah sebaliknya, dari layer paling bawah ke *layer* paling atas. Protokol pada *physical layer* di *host* tujuan mengambil paket data dari media transmisi kemudian mengirimkannya ke data *link layer*, *data link layer* memeriksa *data-link layer header* yang ditambahkan *host* pengirim pada paket, jika *host* bukan yang dituju oleh paket tersebut maka paket itu akan di buang, tetapi jika *host* adalah yang dituju oleh paket tersebut maka paket akan dikirimkan ke *network layer*, proses ini terus berlanjut sampai ke *application layer* di *host* tujuan.

2.4.4. Pengertian TCP/IP

TCP/IP *(Transmission Control Protokol / Internet Protokol)* adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas *(WAN).* TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja.

2.4.5. Definisi Masing-masing Layer pada model TCP/IP

Protokol model TCP/IP terdiri dari empat layer seperti ditunjukkan pada Gambar 2.5.



Gambar 2.5 Model TCP/IP Layer

1) **Application**

Layer application adalah *layer* paling atas pada model TCP/IP, yang bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan jaringan TCP/IP. Protokol ini mencakup protokol *Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP),* dan masih banyak protokol lainnya. Dalam beberapa implementasi *Stack Protocol*, seperti halnya Microsoft TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka *Windows Sockets (Winsock)* atau *NetBios over TCP/IP (NetBT).*

2) **Transport**

Layer transport berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah *Transmission Control Protocol (TCP) dan User Diagram Protocol (UDP).*

3) **Internet**

Layer internet berfungsi untuk melakukan pemetaan (*routing*) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah *Internet Protocol (IP), Address Resolution Protocol (ARP),Internet control Message Protocol (ICMP),* dan *Internet Group Management Protocol (IGMP).*

4) ***Network Interface***

Network interface berfungsi untuk meletakkan frame – frame jaringan di atas media jaringan yang digunakan. TCP/IP dapat bekerja dengan banyak teknologi transport, mulai dari teknologi transport dalam LAN (seperti halnya *Ethernet dan Token Ring*), Man dan Wan (seperti halnya dial-up model yang berjalan di atas *Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN),* serta *Asynchronous Transfer Mode (ATM)*.

2.5. Subnetting

Subnetting adalah proses membagi atau memecah sebuah *network* menjadi beberapa *network* yang lebih kecil atau yang sering disebut *subnet.* Dengan *subnetting*, pengguna dapat menentukan jumlah *host* yang akan digunakan di dalam jaringan. Bila pengguna hanya punya lima *host*, tetapi subnetmask tidak 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. Oleh karena itu, maka perlu menggunakan *subnetting* untuk mengefisiensikan penggunaan *bandwitdh* jaringan (Rafiudin, 2006).

Beberapa manfaat *subnetting* ini antara lain:

1) Mengurangi lalu-lintas jaringan, sehingga data yang lewat di perusahaan tidak akan bertabrakan *(collision)* atau macet.
2) Optimasi kerja jaringan
3) Peyederhanaan pengelolaan jaringan

2.6.*Hotspot*

Hotspot atau area bersinyal adalah lokasi dimana pengguna dapat mengakses melalui mobile komputer tanpa menggunakan koneksi kabel dengan tujuan dapat mengakses suatu jarigan seperti internet. Adapun tujuan dari pembuatan *hotspot* adalah : 1) Turut serta dalam pengembangan internet murah di masyarakat. 2) Membangun komunitas yang sadar akan kehadiran teknologi informasi dan internet. 3) Sharing informasi di lingkungan sekolah atau perumahan sehingga masyarakat lebih mengerti fungsi dari internet.

Hotspot digunakan untuk melakukan autentikasi pada jaringan local. Autentikasi yang digunakan berdasarkan pada HTTP atau HTTPS protocol dan dapat diakses dengan menggunakan *Web Browser*. *Hotspot* sendiri adalah sebuah sistem yang mengkombinasikan beberapa macam fitur dari Mikrotik *Router*OS yang sangat mudah dikonfigurasi. *Hotspot System* adalah sebuah

teknologi autentikasi yang biasa digunakan ketika kita akan menyediakan akses internet pada areal publik, seperti : Hotel, café, airport, taman, mall dll. Teknologi akses internet ini biasanya menggunakan jaringan *wireless* atau *wired*. Kita bisa menyediakan akses internet gratis dengan menggunakan *hotspot* atau bisa juga menggunakan Voucher untuk autentikasinya

Ketika memcoba membuka sebuah *web page* maka *router* yang sudah memiliki *hotspot system*, akan melakukan tes apakah *user* sudah di autentikasi pada sistem *hotspot* tersebut. Jika belum melakukan autentikasi, maka user akan di arahkan pada *hotspot login page* yang harus diisikan berupa *username* dan *password*. Jika informasi *login* yang dimasukkan sudah benar, maka *router* akan memasukkan *user* tersebut kedalam *hotspot* system dan *client* sudah bisa mengakses halaman web. Selain itu akan muncul popup windows berisi status ip address, *byte rate dan time live*. Dari urutan proses diatas, maka user sudah bisa mengakses halaman internet melalui *hotspot gateway*. Keunggulan *hotspot system* digunakan untuk autentikasi user, penggunaan akses internet dapat dihitung berdasarkan waktu dan data yang di-*download / upload*. Selain itu dapat juga dilakukan limitasi bandwidth berdasarkan data *rate*, total data *upload/download* atau bisa juga di limit berdasarkan lama pemakaian dan *system Radius*.

2.7. *Firewall*

Firewall atau *adaptive security appliance* adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *access control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. *Firewall* seperti halnya alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas network dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah seperti yang terlihat.

Firewall digunakan untuk mengontrol akses antara network internal sebuah organisasi internet. Sekarang ini *firewall* semakin menjadi fungsi standar yang ditambahkan untuk semua host yang berhubungan dengan network (Purbo, 2000).

Fungsi-fungsi umum *firewall* adalah sebagai berikut: (a) *Static packet filtering* (penyaringan paket secara statis) (b) *Dynamic packet filtering* (penyaringan paket secara dinamis) (c) *Stateful filtering* (penyaringan paket berdasarkan status) (d) *Proxy*.

2.7.1 Pengertian Paket Filtering

Paket filtering firewall adalah salah satu jenis teknologi keamanan yang digunakan untuk mengatur paket-paket apa saja yang diizinkan masuk ke dalam sistem atau jaringan dan paket-paket apa saja yang diblokir. *Packet filtering* umumnya digunakan untuk memblokir lalu lintas yang mencurigakan yang datang dari alamat IP yang mencurigakan, nomor port TCP/UDP yang mencurigakan, jenis protokol aplikasi yang mencurigakan, dan kriteria lainnya.

Bagian yang diperiksa dari paket data tersebut adalah bagian *header* yang berisi informasi penting, yaitu:

1) IP address sumber
2) IP address tujuan
3) Protokol (TCP/UDP/ICMP)
4) Port sumber dari TCP atau UDP
5) Port tujuan dari TCP atau UDP
6) Tipe pesan dari ICMP
7) Ukuran dari paket

Internet adalah gabungan PC yang dihubungkan melalui *router-router* yang saling terkoneksi dimana setiap PC memiliki alamat yang berbeda-beda (unik). *Firewall* jenis ini bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam Access Control List *firewall*, *router* tersebut akan mencoba memutuskan

apakah hendak meneruskan paket yang masuk tersebut ke tujuannya atau menghentikannya.

2.7.2 Faktor Penting Pendukung Keamanan

Untuk dapat mengimplementasikan system keamanan yang baik, diperlukan faktor penting sebagai berikut.

1) *Perimeter Network*

Adalah sebuah *layer* lain dari *security*. Adalah *layer* yang terletak antara jaringan dalam atau jaringan lokal kita dan jaringan luar atau internet.

2) *Interior Router*

Interior *router* ini kebanyakan melakukan paket filtering *firewall* pada sistem. *Router* ini menyediakan pelayanan *filtering* dari luar dan dari dalam.

3) *Exterior Router*

Exterior router berkewajiban untuk memperbolehkan apa saja yang *outbound* dari *perimeter net* dan biasanya melakukan *paket filtering* yang minim. *Router* ini biasanya disediakan oleh sebuah grup diluar dari jaringan.

2.7.3 Jenis-jenis Paket Filtering

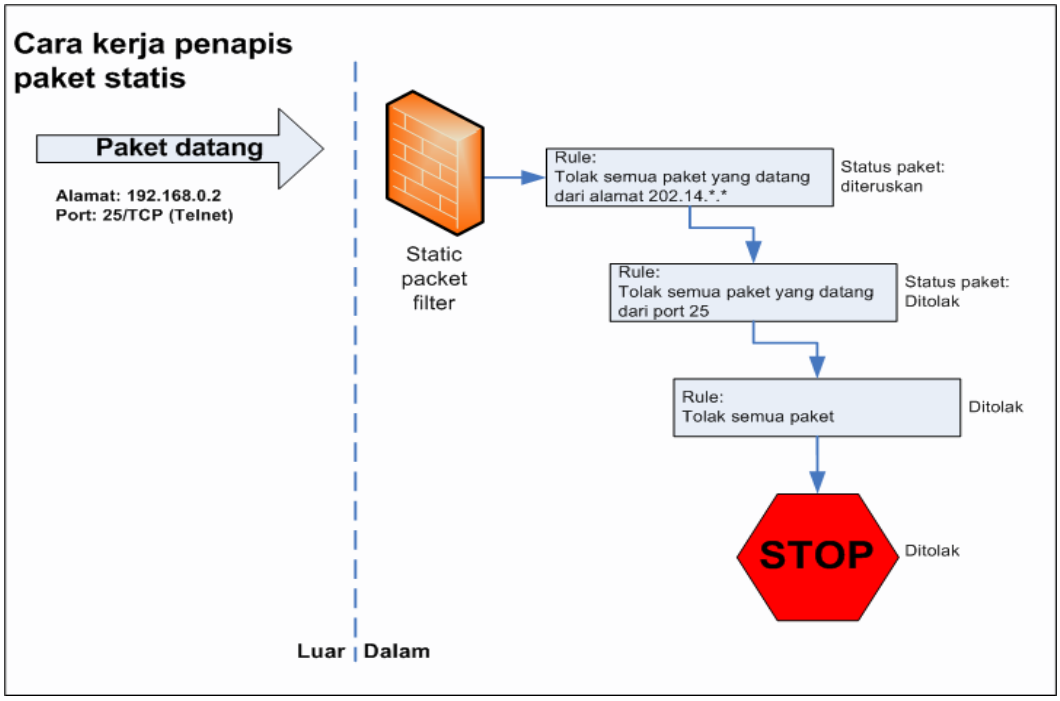
Terdapat dua jenis paket filtering *firewall*, yaitu *Paket filtering statis* dan *paket filtering dinamis*.

1) Paket Filtering Statis

Paket filtering statis ini akan menentukan apakah akan menerima atau memblokir setiap paket berdasarkan informasi yang terdapat pada *header* paket tersebut (seperti IP address sumber dan tujuan, port sumber dan tujuan, dan lain-lain). *Paket filtering statis* ini umumnya terdapat pada sistem operasi dan *router* yang menggunakan tabel daftar pengaturan akses (*access control list*).

IT manager dapat mengelola keamanan jaringannya dengan membuat *policy*/kebijakan. Setiap paket yang filter akan dibandingkan dengan setiap

peraturan yang diterapkan di dalam filter tersebut. Apabila hasil dari perbandingan ini tidak cocok, maka paket tersebut di blok. Namun, apabila sesuai paket tersebuat akan diteruskan. Untuk lebih jelas, perhatikan ilustrasi cara kerjanya pada Gambar 2.6, pada saat paket data datang dengan alamat IP 192.168.0.2 dengan port 25 dan protocol TCP melewati filter, terjadi pengecekan terhadap paket data tersebut. Informasi yang terdapat pada paket data kemudian dibandingkan dengan rule yang terdapat pada *firewall*. Rule pertama adalah tolak semua paket yang berasal dari alamat 202.14.*.* yaitu alamat yang memiliki IP depan 202.14, karena alamat sumber paket bukan merupakan alamat IP dengan angka depan 202.14, maka paket diteruskan pada pemeriksaan dengan rule berikutnya.



Gambar 2.6 Cara Kerja *Paket Filtering Statis*

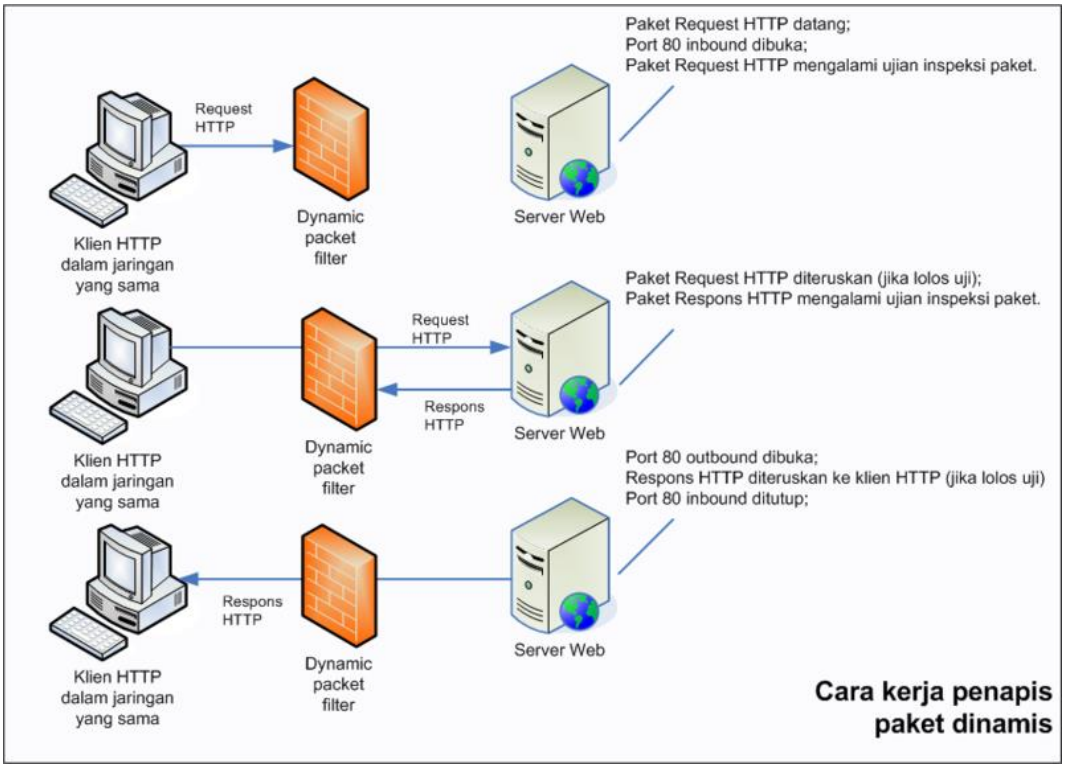
Rule dua menyebutkan tolak semua paket yang berasal dari port 25. Sesuai dengan rule, paket yang datang tadi berasal dari port 25 sehingga, paket data akan di drop atau tidak diteruskan. Begitupun dengan rule tiga. Umumnya perangkat yang memiliki fitur paket filtering, mengizinkan seorang administrator

untuk menerapkan dua jenis peraturan. Pertama, *inbound rule* yaitu pemeriksaan terhadap paket yang akan masuk ke dalam jaringan lokal dari internet, Kedua *outbound rule* yaitu pemeriksaan yang dilakukan terhadap paket yang akan keluar dari jaringan lokal menuju internet.

2) Paket Filtering Dinamis

Paket filtering dinamis bekerja seperti halnya *paket filtering statis*, tetapi pemeriksaan jenis ini juga tetap menjaga informasi sesi yang mengizinkan mereka untuk mengontrol aliran paket antara dua host secara dinamis, dengan cara membuka dan menutup port komunikasi antara keduanya sesuai dengan kebutuhan. Penyaringan seperti ini sering diimplementasikan di dalam *firewall*, dimana *firewall* tersebut dapat digunakan untuk mengontrol aliran data masuk ke jaringan lokal, maupun aliran data yang keluar dari jaringan lokal.

Misalnya, sebuah *paket filtering dinamis* dapat dikonfigurasikan sedemikian rupa sehingga hanya lalu lintas inbound protokol *Hypertext Transfer Protocol (HTTP)* saja yang diizinkan masuk ke jaringan lokal, sebagai respon dari request dari klient HTTP yang berada pada jaringan local. Untuk itu, lalu lintas outbound yang melalui port 80 dengan protokol TCP akan diizinkan, sehingga request HTTP dari klient yang berada pada jaringan lokal dapat diteruskan. Untuk lebih jelas perhatikan Gambar 2.7.



Gambar 2.7 Cara Kerja *Paket Filtering Dinamis*

Ketika sebuah *request HTTP outbound* datang melalui filter, filter ini akan melakukan pemeriksaan terhadap paket tersebut untuk memperoleh informasi sesi TCP dari *request* itu, kemudian filter akan membuka *port 80* untuk lalu lintas inbound sebagai respon terhadap *request* tadi.

Ketika respon HTTP datang, respon tersebut akan melalui *port 80* menuju ke dalam jaringan, dan kemudian filterakan menutup *port 80* untuk lalu lintas *inbound*. Namun, filtering jenis ini dapat di tembus oleh *hacker* dengan membajak sesi dari paket data, sehingga paket data yang dikirim oleh *hacker* tersebut adalah paket data yang diizinkan sesuai dengan rule yang di tetapkan.

2.7.4 Cara Kerja Paket Filtering *Firewall*

Firewall mengawasi paket data yang lewat melalui *router*. *Router* ini dapat berfungsi sebagai sebuah server karena itu *router* ini dituntut untuk dapat memberikan route pada paket yang datang kepadanya. *Router* juga memikirkan bagaimana suatu paket data dapat sampai pada tujuan yang sebenarmya. Dalam hal ini, *router* tersebut saling berkomunikasi melalui protokol untuk memberikan route terhadap paket data yang datang. Protokol ini disebut *Routing Information Protocol (RIP)* yang menghasilkan sebuah tabel routing. Tabel routing inilah yang menunjukkan tujuan paket data akan dikirim.

Pada beberapa sistem, teknik pengamanan jaringan dapat hanya dilakukan dengan memasang *router* filtering dan hanya pada lokasi tertentu saja pada jaringan kita. Oleh karena itu, *router* yang berfungsi sebagai filter harus dapat mengambil keputusan apakah paket berasal dari jaringan lokal atau berasal dari luar (internet), kegiatan ini disebut *source address forgery*.

Seperti yang telah disebutkan sebelumnya, bahwa yang diperiksa dari sebuah paket data adalah bagian *header* nya yang mengandung informasi penting tentang paket tersebut.

1) **Protokol,** informasi yang terdapat pada *header* ini tersusun atas byte-byte. Byte ke 9 merupakan informasi tentang protokol yang digunakan.
2) **Alamat IP Sumber,** adalah IP address sumber yang mengirimkan paket data tersebut (berukuran 32 byte).
3) **Alamat IP Tujuan,** adalah IP address tujuan paket tersebut dikirimkan (berukuran 32 byte).
4) **Port Sumber (TCP/UDP),** adalah port yang menjadi tempat keluarnya paket data pengirim. Pada setiap akhir dari koneksi TCP atau UDP tersambung dengan sebuah port, Walaupun port-port TCP terpisah dan cukup jauh dari port-port UDP. Port-port yang mempunyai nomor dibawah 1024 diterbalikan karena nomor-nomor ini telah didefinisikan secara khusus, sedangkan untuk port-port yang bernomor diatas 1024 (inklusif) lebih dikenal dengan port ephermal. Konfigurasi dari nomor pengalamatan ini diberikan sesuai dengan pilihan dari *vendor*.
5) **Port Tujuan,** adalah port yang menjadi saluran masuk paket data pada komputer penerima paket data.
6) **Status Koneksi,** status koneksi memberitahkan apakah paket data yang dikirimkan adalah paket pertama dari sesi di jaringan. Jika paket merupakan paket pertama maka pada TCP *header* diberlakukan ‘false’ atau 0 dan untuk mencegah sebuah host untuk mengadakan koneksi dengan menolak atau membuang paket yang mempunyai bit set ‘false’ atau 0.

Header pada paket data tersebut kemudian diperiksa, dengan cara membandingkannya dengan policy atau kebijakan yang telah dibuat oleh administrator jaringan. Apabila ada salah satu kebijakan tadi dilanggar, maka paket data yang datang akan di drop.

2.7.5 Keunggulan dan Kelemahan Paket Filtering *Firewall*

Metode paket filtering *firewall* ini memiliki beberapa keunggulan, yaitu :

1) Performa yang tinggi, karena melakukan pengecekan terhadap banyak faktor (port, ip address, dan lain-lain).
2) Dapat diterapkan pada perangkat jaringan biasa *router* atau *switch* tanpa memerlukan perangkat tambahan.
3) Efektif

2.8. *Router*

Router adalah perangkat keras yang memfasilitasi transmisi paket data melalui jaringan komputer. "*Router* merupakan perangkat jaringan yang bekerja pada OSI layer 3"(Citraweb Nusa Infomedia, 2016). Fungsi *router* adalah sebagai penghubung antara dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. *Router* berbeda dengan *switch*. Sebagai ilustrasi perbedaan fungsi *router* dan *switch* adalah *switch* merupakan sebuah jalan, dan *router* merupakan penghubung antar jalan. Masing-masing rumah berada pada jalan yang memiliki alamat dalam suatu urutan tertentu.

2.9. Sejarah Mikrotik

Mikrotik *Router*OS™ 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 berimigrasi 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). Prinsip dasar mereka bukan membuat *Wireless* ISP (WISP), tapi membuat program *router* yang handal dan dapat dijalankan di seluruh dunia (Herlambang, 2009).

2.9.1 Pengertian Mikrotik

Mikrotik merupakan sistem operasi *linux base* yang dirancang secara khusus untuk keperluan *networking*. Didesain untuk memberikan kemudahan

bagi penggunanya. 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 Komputer)* (Ari Sujarwo, 2009).

PC yang akan dijadikan *router* mikrotik pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standard, misalnya sebagai *gateway* dan manajemen *bandwidth*. Untuk keperluan beban yang besar disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai (Kustanto, 2008).

2.9.2 Jenis Mikrotik

Jenis-jenis mikrotik yang tersedia adalah sebagai berikut :

1) *Mikrotik Router OS* adalah versi *mikrotik* dalam bentuk perangkat lunak yang dapat diinstal pada komputer rumahan (PC) melalui CD. Untuk dapat menggunakannya secara *full time*, harus membeli *licensi key* dengan catatan satu lisensi hanya untuk satu *harddisk*.
2) *Build In Hardware Mikrotik*, merupakan *mikrotik* dalam bentuk perangkat keras yang khusus dikemas dalam *router board* yang di dalamnya sudah terinstal *Mikrokik Router OS*. Untuk versi ini, lisensi sudah termasuk dalam *board mikrotik* (Aziz dan Herlambang, 2009).

2.9.3 Mikrotik sebagai *Firewall*

Firewall berfungsi menjaga keamanan jaringan dari ancaman pihak lain yang tidak berwenang. Mengubah, merusak, atau menyebarkan data-data penting perusahaan merupakan contoh ancaman yang harus dicegah.

Firewall beroperasi menggunakan aturan tertentu. aturan inilah yang menentukan kondisi ekspresi yang memberitahu *router* tentang apa yang harus dilakukan *router* terhadap paket IP yang melewatinya. Setiap aturan disusun atas kondisi dan aksi yang akan dilakukan. Ketika ada paket *IP* lewat, *firewall* akan mencocokkannya dengan kondisi yang telah dibuat kemudian menentukan aksi apa yang akan dilakukan *router* sesuai dengan kondisi tersebut (Rafiudin, 2006).

Selain sebagai *gateway*, *mikrotik* juga dipadukan dengan kemampuan *firewall* untuk mencegah hal-hal yang menggangu dari pihak lain, mengingat begitu banyaknya aplikasi yang dijalankan oleh pengguna jaringan. Ada aplikasi yang berjalan normal, tetapi ada juga aplikasi yang bersifat mengganggu kinerja jaringan. Sebagai contoh, paket *broadcast* yang dilakukan oleh *virus* dan paket berlebihan yang sering disebut sebagai *flooding*. Paket dengan ukuran kecil memang tidak mengganggu koneksi jaringan. Namun, jika paket yang kecil tersebut dalam jumlah banyak, hal ini bisa menurunkan kinerja jaringan (*down*). Maka disinilah pentingnya memakai *firewall* untuk menghindari insiden jaringan yang bersifat negatif.

Pada sistem operasi Mikrotik, *firewall* sudah termasuk paket Mikrotik *Router*OS yang di dalam direktori *firewall* sendiri terdapat 6 direktori:

1. *Mangle*, untuk menandai paket dengan suatu tanda khusus sebagai indentitas paket tersebut.

2. *NAT*, ntuk memetakan suatu *IP address* ke *IP address* lain.

3. *Connection*, untuk mengetahui informasi dari suatu koneksi yang aktif, seperti *IP address* asal dan tujuan beserta *port* yang digunakan, jenis protokol yang dipakai.

4. *Address-list*, untuk mendefinisikan *IP address* ke dalam group tertentu. *Service port*, untuk mengaktifkan dan mengubah nomor *port* aplikasi.

5. *Filter*, untuk menyaring paket yang masuk atau melewati *router*. *Router* akan meneruskannya jika paket diizinkan lewat, dan sebaliknya.

6. *Export*, untuk menyimpan/*backup* semua konfigurasi di dalam direktori *firewall*.

2.9.4 Network Address Translator (NAT)

Untuk memecahkan persoalan alamat ini, para desainer *internet* mencadangkan suatu bagian dari ruang alamat *IP* dan menamai ruang ini sebagai ruang alamat pribadi. Suatu alamat *IP* pada ruang alamat pribadi tidak pernah diberikan sebagai alamat umum. Alamat *IP* di dalam ruang alamat pribadi

dikenal sebagai alamat pribadi. Dengan memakai alamat *IP* pribadi, kita dapat memberikan proteksi dari para *hacker* jaringan (Fajar Gunawan, 2009).

Karena alamat *IP* pada ruang alamat pribdi tidak akan pernah diberikan oleh *Internet Network Information Center (InterNIC*) sebagai alamat umum, maka *route* di dalam *internet router* untuk alamat pribadi takkan pernah ada. Alamat pribadi tidak dapat dijangkau di dalam *internet*. Oleh karena itu, saat memakai alamat IP pribadi, kita membutuhkan beberapa tipe *proxy* atau *server* untuk mengonversi sejumlah alamat IP pribadi pada jaringan lokal kita menjadi alamat IP umum yang dapat di-*routed* (Herlambang, 2009).

Pilihan lain adalah menerjemahkan alamat pribadi menjadi alamat umum yang *valid* dengan *network address translator (NAT)* sebelum dikirimkan di *internet*. Dukungan bagi *NAT* untuk menerjemahkan alamat umum dan alamat pribadi memungkinkan terjadinya koneksi jaringan-jaringan kantor-rumah atau kantor yang kecil ke *internet.*