

BAB 2

TINJAUAN PUSTAKA

2.1 Profil Tempat Penelitian

SMA Negeri 27 Bandung, merupakan salah satu Sekolah Menengah Atas Negeri yang ada di Bandung. Saat ini SMA Negeri 27 Bandung sudah memiliki gedung sendiri yang beralamat di Jalan Utsman Bin Affan No. 1 Kel. Rancanumpang Kec. Gedebage - Bandung, Jawa Barat. Sama dengan SMA pada umumnya di Indonesia masa pendidikan sekolah di SMA Negeri 27 Bandung ditempuh dalam waktu tiga tahun pelajaran, mulai dari Kelas X sampai Kelas XI. Sejak berdirinya pada tahun 2006 hingga sekarang SMA Negeri 27 Bandung telah dipimpin oleh 7 orang kepala sekolah, dimana awal berdirinya SMA Negeri 27 berada dilingkungan SMA Negeri 2 yang berada di Jalan Cihampelas Kecamatan Coblong. Sesuai dengan perkembangan dan kebijakan Pemerintah Daerah Kota Bandung di tahun ke 6 lokasi berpindah ke alamat baru yaitu Jalan Utsman bin Affan No. 1 Kel. Rancanumpang Kecamatan Gedebage Bandung.



Gambar 2.1 Logo SMAN 27 Bandung

2.1.1 Visi dan Misi

Visi dan misi dari SMA Negeri 27 Bandung adalah sebagai berikut:

1. Visi
 - a. Unggul dan berprestasi dalam pengamalan nilai-nilai agama
 - b. Unggul dan berprestasi dalam proses pembelajaran.
 - c. Unggul dan berprestasi dalam hasil belajar (akademis).

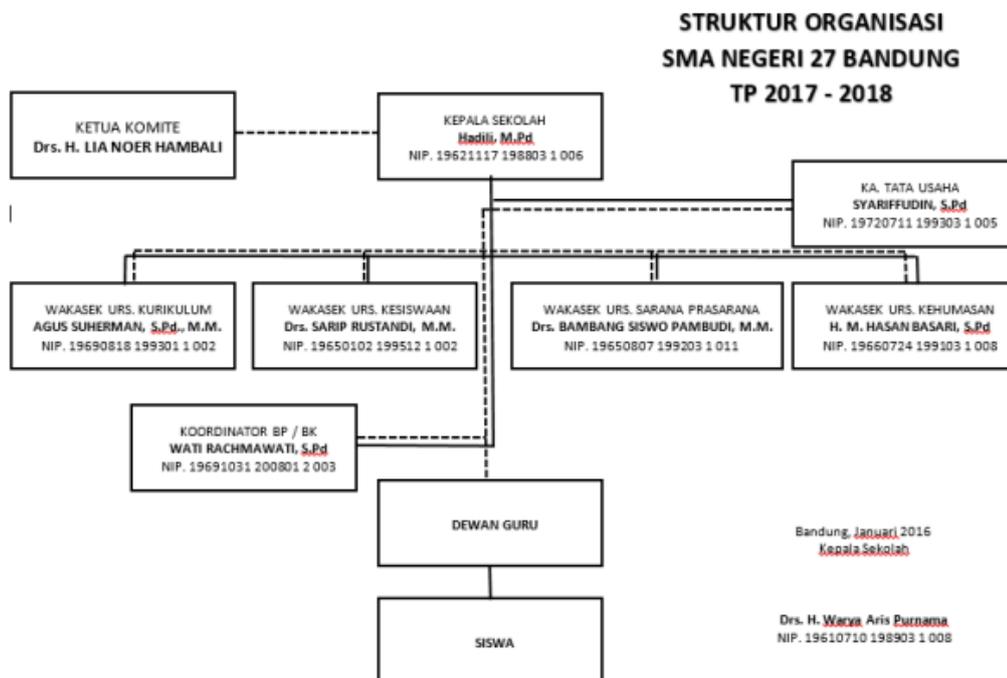
- d. Unggul dan berprestasi dalam kelanjutan pendidikan di Perguruan Tinggi.
- e. Unggul dan berprestasi dalam persaingan hidup (mandiri)
- f. Unggul dan berprestasi dalam mengimplementasikan nilai-nilai budaya.
- g. Unggul dan berprestasi dalam bidang olahraga, seni dan budaya.
- h. Unggul dan berprestasi dalam penguasaan dan pemanfaatan ilmu pengetahuan dan teknologi
- i. Unggul dalam menegakkan nilai-nilai kesadaran terhadap kedisiplinan (hukum)
- j. Unggul dalam kepedulian terhadap lingkungan

2. Misi

- a. Meningkatkan kekuatan keimanan dan ketakwaan terhadap Tuhan YME
- b. Meningkatkan kemampuan penguasaan IPTEK;
- c. Membentuk peserta didik yang kreatif dan inovatif
- d. Menyiapkan peserta didik yang mampu bersaing dalam melanjutkan pendidikan ke jenjang yang lebih tinggi
- e. Meningkatkan nilai-nilai budi pekerti luhur disertai kesadaran ketaatan terhadap hukum (aturan)
- f. Meningkatkan kesadaran untuk memiliki sifat kekeluargaan dan kebersamaan
- g. Mengelola kurikulum dan pembelajaran yang berorientasi pengembangan mutu
- h. Membina siswa melalui kegiatan pengembangan diri dan konseling berdasarkan bakat dan minat untuk mengoptimalkan potensi diri
- i. Melatih dan membina profesionalisme guru dan tenaga kependidikan.
- j. Melengkapi sarana dan prasarana sekolah pendukung proses pendidikan

- k. Menciptakan suasana dan lingkungan pendidikan yang kondusif untuk mendukung efisiensi pembelajaran.
- l. Mewujudkan lingkungan sekolah yang hijau, asri dan lestari
- m. Menjalin kemitraan dengan berbagai lembaga yang mendukung keberhasilan pendidikan
- n. Menjadi sekolah yang mengakomodasi masyarakat dalam rangka mewujudkan program wajib belajar tingkat SMA (Program Wajib Belajar 12 Tahun)

2.1.2 Struktur Organisasi



Gambar 2.2 Struktur Organisasi SMAN 27 Bandung

2.1.3 Deskripsi Kerja SMAN 27 Bandung

Saat ini SMA Negeri 27 Bandung memiliki bidang kerja dan pegawai. adapun pegawai ialah mulai dari level komite sekolah sampai ke siswa. Dan berikut ini penjelasan mengenai fungsi pokok dari masing-masing bidang yang di deskripsikan sebagai berikut:

1. Komite Sekolah.

Komite Sekolah adalah suatu lembaga mandiri yang di bentuk dan berperan dalam peningkatan mutu pelayanan dengan memberikan pertimbangan, arah dan dukungan tenaga, sarana, dan prasarana.

2. Kepala Sekolah

Kepala sekolah adalah guru yang diberikan tugas tambahan untuk memimpin suatu sekolah yang diselenggarakan proses belajar-mengajar atau tempat terjadi interaksi antara guru yang memberi pelajaran dan murid yang menerima pelajaran.

3. Tata Laksana

Tata Laksana adalah satuan usaha kegiatan pengelola surat-menyurat yang di mulai dari menerima, mencatat, mengelola dan mengirim semua bahan keterangan yang di perlukan organisasi

4. Wakil Kepala Sekolah

Wakil Kepala Sekolah bertugas untuk membantu kepala sekolah dalam urusan: kurikulum, kesiswaan, sarana prasarana dan humas.

5. Staf

Staf merupakan tenaga struktural (non Fungsional) yang bertugas untuk membantu berjalanya organisasi dengan baik.

6. Korbid

Koordinator bidang adalah seorang yang di tunjuk untuk bertanggung jawab menjalankan bidang yang berada dalam organisasi tersebut.

7. Wali Kelas

Wali kelas adalah guru yang membantu kepala sekolah untuk membimbing siswa dalam mewujudkan disiplin kelas, sebagai motivator untuk membangkitkan minat siswa di kelas.

8. MGMP

Musyawarah Guru Mata Pelajaran adalah suatu organisasi yang di bentuk untuk menggambarkan pembelajaran profesionalisme guru.

9. Guru

Guru adalah seorang pengajar suatu ilmu, guru bertugas untuk mendidik, mengajar, membimbing, mengarahkan, melatih, menilai dan mengevaluasi peserta didik

10. Divisi ICT

Divisi ICT adalah divisi khusus yang bertugas untuk membantu kepala sekolah untuk manajemen komputerisasi yang berjalan di SMA Negeri 27 Bandung.

2.2 Landasan Teori

Berikut ini adalah beberapa landasan teori yang digunakan oleh penulis sebagai pendukung teori dasar dari “Penerapan *Transparent DNS*, Pencegahan Penggunaan *Proxy* dan VPN Menggunakan *Firewall* dengan Metode *Layer 7 Protocol* Mikrotik Untuk Optimalisasi *Filtering* Konten Negatif Serta Implementasi di SMAN 27 Bandung”.

2.2.1 Jaringan Komputer

Jaringan komputer merupakan dua atau lebih sistem komputer yang terpisah, melalui media komunikasi untuk melakukan komunikasi data satu dengan yang lain guna berbagi sumber daya.

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. Dua buah komputer misalnya dikatakan terkoneksi bila keduanya dapat saling bertukar informasi.

Berdasarkan Pengertian tersebut dapat di simpulkan bahwa jaringan komputer adalah sistem yang terpisah untuk melakukan komunikasi agar dapat bertukar informasi. [2]

2.2.1.1 Manfaat Jaringan Komputer

Adapun manfaat yang didapat dalam membangun jaringan komputer adalah sebagai berikut. [2]

- a. *Sharing Resource*, bertujuan agar seluruh program, peralatan lainnya dapat dimanfaatkan oleh setiap orang yang ada pada jaringan komputer tanpa terpengaruh oleh lokasi maupun pemakaian.
- b. Media komunikasi, jaringan komputer memungkinkan terjadinya hubungan antara komputer pengguna, baik untuk *teleconference* maupun untuk mengirim pesan atau informasi penting lainnya. Dengan menggunakan

jaringan komputer dua orang atau lebih yang jaraknya sangat jauh akan lebih mudah bekerja.

c. Integrasi data, pembangunan jaringan komputer dapat mencegah ketergantungan pada komputer pusat, setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke tempat lainnya.

d. Pengembangan dan pemeliharaan, dengan adanya jaringan komputer ini, maka pengembangan peralatan dapat dilakukan dengan mudah dan menghemat biaya. Jaringan komputer juga bisa memudahkan pemakai dalam merawat *hard disk* dan peralatan lainnya, seperti memberikan perlindungan terhadap serangan virus maka pemakai cukup memusatkan perhatian pada *hard disk* yang ada di komputer pusat.

e. Keamanan data, memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melalui pengaturan hak akses para pemakai dan *password*, serta teknik perlindungan terhadap *hard disk* sehingga data mendapatkan perlindungan yang efektif.

2.2.1.2 Klasifikasi Jaringan Komputer

Pengklasifikasian jaringan komputer secara garis besar terdiri dari klasifikasi utama yaitu: [2]

1. Berdasarkan Topologi

Topologi jaringan adalah bagaimana jaringan itu tersambung secara fisik atau logika. Model topologi yang umum dibangun saat ini adalah star, bus, ring, mesh, P2P, dan tree topologi. Selain model tersebut masih terdapat model lainnya

2. Berdasarkan geografis

Cakupan geografis jaringan komputer secara umum dibagi atas tiga jenis, yaitu:

a. *Local Area Network*

LAN (Local Area Network) merupakan satuan terkecil dari jenis cakupan jaringan komputer, contohnya jenis jaringan LAN adalah jaringan internal kampus/sekolah, kantor, warung internet.

b. *Metropolitan Area Network*

MAN (Metropolitan Area Network) merupakan satuan menengah dari jenis cakupan jaringan komputer, contoh jaringan MAN adalah jaringan publik diimplementasikan di dalam satu kota.

c. *Wide Area Network*

WAN (Wide Area Network) merupakan cakupan terluas dari jenis cakupan jaringan komputer lainnya. Jaringan ini disamakan dengan jaringan internet, karena lingkungannya yang begitu luas, hingga jaringan antar kota, negara, bahkan benua.

3. Berdasarkan Fungsi

a. Desentralisasi (Tersebar/Terdistribusi)

Sistem yang terdiri atas sejumlah komputer yang tersebar pada berbagai lokasi yang dihubungkan dengan sarana telekomunikasi dengan masing-masing komputer mampu melakukan pemrosesan yang serupa secara mandiri, tetapi bisa saling berinteraksi dalam pertukaran data.

b. Sentralisasi (Terpusat)

Semua pemrosesan data dilakukan oleh komputer yang ditempatkan di dalam suatu lokasi yang ditujukan utk melayani semua pemakai dalam organisasi. Banyak digunakan oleh perusahaan yang tidak memiliki cabang.

c. *Client / Server*

Sembarang sistem atau proses yg melakukan sesuatu permintaan data atau layanan ke *server*. Mempunyai kemampuan untuk melakukan proses sendiri. Sistem ini lebih cocok jika disebut dengan sistem pelayanan antara *customer (client)* dengan *customer service (Server)* dan disini ada timbal balik informasi dimana ketika *customer* meminta

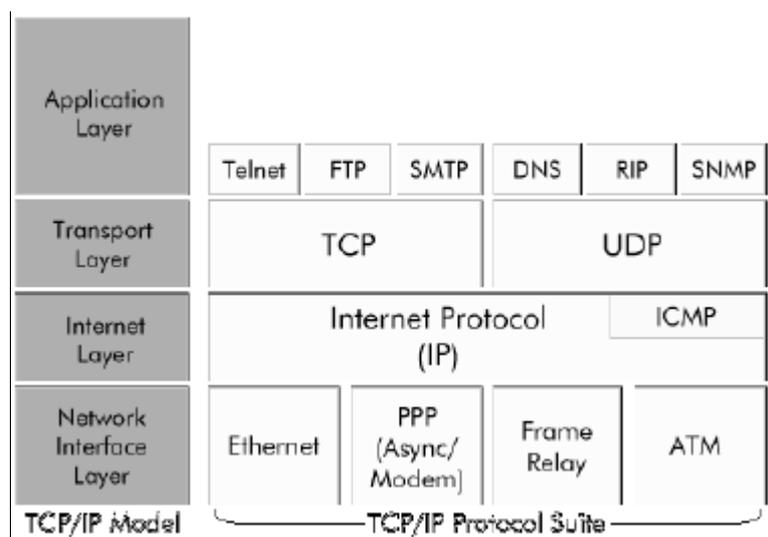
informasi maka *customer service* memberikan apa yang diminta oleh *customer*.

2.2.2 Protokol Jaringan

Di dalam jaringan komputer, komunikasi terjadi antara sekumpulan entitas yang berbeda. Entitas adalah sesuatu yang mampu mengirim atau menerima informasi. Namun, dua entitas tidak begitu saja mengirim aliran bit data satu sama lain dan dapat dipahami. Untuk terjadinya komunikasi, entitas harus menyetujui suatu protokol. Protokol adalah seperangkat aturan yang mengatur komunikasi data. Protokol mendefinisikan apa itu komunikasi, bagaimana berkomunikasi dan apa yang terjadi ketika berkomunikasi.

2.2.2.1 TCP/IP Protocol Suite

TCP/IP protocol suite dikembangkan sebelum model OSI. Oleh karena itu, lapisan di TCP/IP protocol suite tidak sama persis dalam model OSI. TCP/IP protocol suite memiliki empat lapisan yaitu network, Internet, transport, dan application. Namun, ketika TCP / IP dibandingkan dengan OSI dapat dikatakan bahwa lapisan network setara dengan gabungan dari layer data link dan physical. Internet layer setara dengan layer network, dan applicaton layer mengerjakan pekerjaan yang sama seperti session, presentation, dan application layer. [3]



Gambar 2.3 TCP/IP Protocol Suite

Sumber: <https://www.distributednetworks.com>

Penjelasan Gambar 2.4 tentang TCP/IP Protocol Suite sebagai berikut: [3]

a. Application layer

Merupakan lapisan dalam arsitektur TCP/IP yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Karena itu terdapat banyak protokol pada lapisan ini, sesuai dengan banyaknya aplikasi TCP/IP yang dapat dijalankan. Contohnya adalah SMTP (Simple Mail Transfer Protocol) untuk pengiriman e-mail, dan FTP (File Transfer Protocol) untuk transfer file.

b. Transport layer

Mendefinisikan cara untuk melakukan pengiriman data antara end to end secara handal. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima adalah sama dengan informasi yang dikirimkan pada pengirim.

c. Internet layer

Mendefinisikan bagaimana hubungan dapat terjadi antara dua pihak yang berada pada jaringan yang berbeda seperti lapisan network pada OSI. Pada jaringan Internet yang terdiri atas puluhan juta host dan ratusan ribu jaringan lokal, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya dimana pun berada. Oleh karena itu, lapisan ini memiliki peranan penting terutama dalam mewujudkan interworking yang meliputi wilayah luas (worldwide Internet).

d. Network layer

Berfungsi yang mirip dengan lapisan Data-Link pada OSI. Lapisan ini mengatur penyaluran data frame data pada media fisik yang digunakan secara handal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 jaringan public, Ethernet untuk jaringan Ethernet, AX.25 untuk jaringan paket radio.

Metode pengalamatan pada *layer* aplikasi disediakan oleh *host*, metode penamaan ini mengizinkan *host* untuk dikonfigurasi dengan nama yang mudah diingat. Sistem pengalamatan ini yang dapat langsung dilihat oleh pengguna.

Nomor *port* merupakan metode pengalamatan yang disediakan di *layer host to host*. Nomor ini digunakan untuk menggambarkan *interface* dari *software* yang akan memproses pada sebuah *host*. [3]

IP address digunakan untuk metode pengalamatan *layer internet*. Saat ini banyak digunakan IP Versi 4, menggunakan *32 bit biner* dan sistem bilangan yang digunakan adalah bilangan desimal. [3]

MAC address merupakan metode pengalamatan di *layer network access*, Dikenal pula dengan istilah *hardware address*. Menggunakan 48 bit biner atau 12 digit hexadecimal [3]

Tabel 2.1 Metode Pengalamatan TCP/IP

| Metode Pengalamatan Arsitektur TCP/IP | |
|---------------------------------------|--------------------------------|
| Arsitektur TCP/IP | Metode Pengalamatan |
| Process/ Application | Nama Host (Host Name) |
| Host-to-host | Nomor Port(Port Number) |
| Internet | Alamat IP (Ip Address) |
| Network Access | Hardware Address (Mac Address) |

Diantara keempat metode pengalamatan tersebut, metode pengalamatan *TCP/IP* yang sering digunakan yaitu *IP address*. Setiap *device* yang terhubung ke jaringan *TCP/IP* membutuhkan paling sedikit satu *IP address* yang bersifat unik, tidak boleh ada dua atau lebih *IP address* yang sama dalam satu jaringan. Sebuah alamat *IP address* terdiri dari dua bagian, yaitu : [3]

a. *Network ID*

Network ID merupakan identitas alamat dari sebuah jalur. Semua *device* yang terhubung pada jalur fisik yang sama harus memiliki *network ID* yang sama. *Network ID* harus unik (tidak diperkenankan memberi alamat *network ID* yang sama pada jalur/segment yang berbeda).

b. *Host ID*

Host ID Merupakan identitas bagi *Host (Workstation, server, interface router dan device lain yang terhubung ke jaringan TCP/IP)*. Dari sisi penggunaannya, alamat *IP* terbagi dalam dua jenis yaitu:

1. *IP Private*

IP Address yang digunakan pada jaringan privat tidak digunakan pada jaringan publik. *IP Address* yang termasuk dalam kelas tersebut dapat di lihat pada tabel 2.2:

Tabel 2.2 Kelas *IP Private*

| Kelas IP | Segmen 1 | Segmen 2 | Segmen 3 | Segmen 4 |
|----------|----------|----------|----------|----------|
| Kelas A | 10 | 1-255 | 1-255 | 1-255 |
| Kelas B | 172 | 16-31 | 1-255 | 1-255 |
| Kelas C | 192 | 168 | 1-255 | 1-255 |

2. *IP Public*

Ip Address yang biasa digunakan pada jalur *public* dan penggunaannya harus melalui proses registrasi dahulu. Alamat *Ip* terbagi kedalam lima kelas yaitu A, B,C, D, dan E. Nilai pada oktet pertama menentukan kelas dari sebuah *IP Address*. Kelas *IP public* dapat di lihat pada table 2.3.

Tabel 2.3 Kelas *IP Publik*

| Kelas IP | Segmen 1 | Segmen 2 | Segmen 3 | Segmen 4 |
|----------|----------|----------|----------|----------|
| Kelas A | 1-126 | 1-255 | 1-255 | 1-255 |
| Kelas B | 128-191 | 1-255 | 1-255 | 1-255 |
| Kelas C | 192-223 | 1-255 | 1-255 | 1-255 |
| Kelas D | 224-239 | 1-255 | 1-255 | 1-255 |
| Kelas E | 240-255 | 1-255 | 1-255 | 1-255 |

2.2.3 Perangkat Jaringan

Perangkat jaringan sangatlah dibutuhkan dalam membangun sistem konfigurasi ini, karena sistem konfigurasi yang akan dibangun ini membutuhkan beberapa perangkat jaringan yang digunakan untuk menghasilkan sistem yang lengkap sesuai dengan yang dibutuhkan oleh pengguna. Adapun perangkat jaringan yang digunakan dalam pembangunan sistem ini adalah sebagai berikut.

2.2.3.1 Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless. [4]

Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

Berbagai fitur ditawarkan pada mikrotik diantaranya : [4]

- a. Firewall dan NAT
- b. Routing – Static routing
- c. Data Rate Management
- d. Hotspot
- e. Point-to-Point tunneling protocols
- f. Simple tunnels
- g. IPsec
- h. Web proxy
- i. Caching DNS client
- j. DHCP
- k. Universal Client
- l. VRRP
- m. UPnP
- n. NTP
- o. Monitoring/Accounting
- p. SNMP
- q. MNDP
- r. Tools

a. Jenis Mikrotik

1. Mikrotik RouterOS

Mikrotik RouterOS adalah sebuah sistem operasi jaringan berbasis UNIX yang memungkinkan untuk bisa menjadikan komputer biasa mempunyai kemampuan seperti halnya router, firewall, bridge, hotspot,

proxy server dan lain sebagainya. Sistem operasi ini sangat ringan dan hanya membutuhkan spesifikasi peraskat keras yang rendah untuk bisa menjalankannya. Untuk itu banyak orang menggunakan sistem operasi ini untuk membangun router pada jaringan mereka. kestabilan dan kemudahan yang ditawarkan oleh mikrotik routerOS membuat banyak perusahaan-perusahaan besar dan lembaga pendidikan berbasis networking menggunakan mikrotik sebagai dasar dan standar untuk router. [4]

Berikut adalah kelebihan yang ditawarkan oleh mikrotik RouterOS [4]

- a. Mikrotik RouterOS mampu merubah komputer biasa (PC) sebagai router yang handal dan berkwalitas.
- b. Berbasis linux sehingga sangat ringan untuk digunakan.
- c. Diinstall sebagai sistem operasi
- d. Biasanya diinstall pada power PC.

2. RouterBoard

RouterBoard adalah sebuah perangkat keras jaringan komputer yang dikembangkan oleh mikrotik yang didalamnya terinstall sistem operasi mikrotik RouterOS. RouterBoard seperti halnya komputer, tetapi RouterBoard memiliki ukuran yang sangat kecil dan praktis. Didalam RouterBoard juga terdapat Processor, RAM, ROM dan memory flash. [4]

Pada Routerboard juga tersedia mulai low-end sampai dengan hight-end Router. Product dari mikrotik RouterBoard yang akan digunakan untuk membangun sistem ini adalah Routerboard Mikrotik RB951Ui-2HND.

b. Lisensi Mikrotik

Lisensi Mikrotik tersedia dari level 0,1,3 sampai dengan level 6, yang jelas kemampuannya berbeda-beda sesuai dengan levelnya, berikut penjelasan lisensi level mikrotik yang ada : [4]

- a. Level 0 : Pada level ini adalah level Demo, jadi tidak ada biaya yang harus dikeluarkan alias gratis. Namun ada batasan bagi penggunaanya dan batasan tersebut hanya dua puluh empat jam, setelahnya level ini akan notresponding secara otomatis.

- b. Level 1 : Level ini sama dengan level 0, masih Demo dan tentunya gratis. Disini anda bisa menggunakannya untuk fungsi routing yang standar saja masih baku dengan satu panel pengaturan dan tidak memiliki batasan waktu penggunaan.
- c. Level 3 : Untuk level ini masih gratis juga, fiturnya sudah termasuk level 1 ditambah dengan kemampuan manajemen perangkat keras Ethernet dan perangkat wireless client serta perangkat kartu jaringan lainnya.
- d. Level 4 : Di level yang ke 4 ini sudah berbayar Harganya sekitar 31 dolar setara dengan Rp. 403.000, fitur ini sudah mencakup level 1,3 dan kemampuan mengelola perangkat wireless akses poin.
- e. Level 5 : Untuk mikrotik level ini harganya 65 dolar setara dengan Rp. 845.000,- fitur ini mencakup level 1,3,4 dan ditambah pengelolaan hotspot yang lebih banyak.
- f. Level 6 : Pada level ini tentunya sudah mencakup semua level atau tidak ada limitnya. Untuk harganya sekitar 155 dolar setara dengan Rp 2.015.000,- kemampuannya sudah mencakup semua level dan dalam batas maksimal.

2.2.4 Winbox

Winbox adalah sebuah *software* atau *utility* yang di gunakan untuk meremote sebuah *server mikrotik* kedalam mode *GUI (Graphical User Interface)* melalui *operating system windows*. Kebanyakan teknisi banyak mengkonfigurasi *mikrotik os* atau *mikrotik routerboard* menggunakan *winbox* di banding dengan yang mengkonfigurasi langsung lewat mode *CLI (Command Line Interface)*. Hal ini karena menggunakan *winbox* dirasa lebih mudah dan simple dibanding melalui *browser*. Dan hasilnya pun juga lebih cepat. [5]

Fungsi dari *winbox* ini banyak sekali. *Winbox* mudah di *install* mudah dipakai, ringan cepat dan tepat. Jika ingin diperinci bisa dilihat dibawah ini. [5]

1. *Setting mikrotik router* dalam mode *GUI*
2. *Setting bandwidth* jaringan internet

3. *Memblokir* sebuah *website/situs*
4. Mempercepat pekerjaan
5. Dan masih banyak yang lainnya.

2.2.4 Firewall

Firewall adalah perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan tersebut maka firewall berperan dalam melindungi jaringan dari serangan yang berasal dari jaringan luar (outside network).

Firewall mengimplementasikan packet filtering dan dengan demikian menyediakan fungsi keamanan yang digunakan untuk mengelola aliran data ke, dari dan melalui router. Sebagai contoh, firewall difungsikan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang datang dari Internet. Selain untuk melindungi jaringan, firewall juga difungsikan untuk melindungi komputer user atau host (host firewall). [6]

Firewall digunakan sebagai sarana untuk mencegah atau meminimalkan risiko keamanan yang melekat dalam menghubungkan ke jaringan lain. Firewall jika dikonfigurasi dengan benar akan memainkan peran penting dalam penyebaran jaringan yang efisien dan infrastruktur yang aman. MikroTik RouterOS memiliki implementasi firewall yang sangat kuat dengan fitur termasuk: [6]

- a. stateful packet inspection
- b. Layer-7 protocol detection
- c. peer-to-peer protocols filtering
- d. traffic classification by:
 - e. source MAC address
 - f. IP addresses (network or list) and address types (broadcast, local, multicast, unicast)
 - g. port or port range
 - h. IP protocols
 - i. protocol options (ICMP type and code fields, TCP flags, IP options and MSS)

- j. interface the packet arrived from or left through
- k. internal flow and connection marks
- l. DSCP byte
- m. packet content
- n. rate at which packets arrive and sequence numbers
- o. packet size
- p. packet arrival time
- q. dll

2.2.4.1 NAT

NAT (*Network Address Translation*) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (*security*), dan kemudahan serta fleksibilitas dalam administrasi jaringan; Jaringan yang didisain untuk menyederhanakan *IP address* dan berperan juga untuk melindungi jaringan. NAT merupakan teknologi yang memungkinkan jaringan *IP Private, software* yang melakukan NAT yang memungkinkan seluruh koneksi rumahan berbagi koneksi internet melalui satu *IP address*. NAT berlaku sebagai penerjemah antara dua jaringan. Dalam beberapa kasus pada jaringan rumahan, posisi NAT diantara jaringan internet dan jaringan lokal Anda. Internet sebagai sisi "*Public*" dan jaringan lokal sebagai sisi "*Private*". Ketika komputer pada jaringan *private* menginginkan data dari jaringan *public* (internet), maka perangkat NAT membuka sedikit saluran antara komputer dan komputer tujuan. Ketika komputer pada jaringan internet membalikkan hasil dari permintaan, yang dilewati melalui perangkat NAT kepada komputer peminta, sehingga paket tersebut dapat diteruskan melewati jaringan *public*. dapat membagi koneksi akses internet. [6]

2.2.4.2 Layer 7 Protocol

Layer 7 Protocol adalah *layer* aplikasi yang berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan dari paket data yang melewati jalur ICMP, TCP dan UDP. [6]

Cara kerja L7 adalah mencocokkan (*matcher*) 10 paket koneksi pertama atau 2KB koneksi pertama dan mencari pola/*pattern* data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, *matcher* tidak memeriksa lebih lanjut. Dan akan dianggap *unknown connections*. Kita harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada *RouterBoard* maupun *PC Router*. [6]

2.2.5 DNS (Domain Name System)

Setiap *network interface* yang terhubung pada *TCP/IP network* diidentifikasi melalui alamat IP. Suatu nama (*hostname*) juga dapat diberikan pada setiap perangkat yang memiliki alamat IP seperti: *server*, *router*, *terminal*, dan sebagainya. Perangkat lunak jaringan tidak memerlukan nama untuk berhubungan. Namun demikian, manusia sebagai pengguna *network* memerlukannya karena lebih mudah diingat dan diketik dengan tepat daripada alamat IP yang diperlukan komputer. Penamaan setiap komputer yang terhubung satu sama lain. Pada Internet, setiap perangkat diberi nama yang informatif. Dengan melihat nama suatu perangkat, minimal orang dapat membayangkan dimana perangkat berada dan *service* apa yang diberikan. Bentuk *hostname* yang digunakan pada Internet mirip dengan alamat IP, yakni terdiri dari beberapa segmen. Setiap segmen berupa nama atau singkatan yang memberikan informasi.

Hubungan setiap segmen berupa hirarki / tingkatan. Segmen disebelah kiri lebih spesifik daripada yang disebelah kanan, atau berada dalam domain nama yang ada pada sebelah kanan. Perhatikan *hostname* dari salah satu perangkat ini: ns1.ts.ac.id

Interpretasi dari nama di atas adalah suatu perangkat yang diberi nama ns1, sesuai dengan namanya yang berfungsi sebagai name server. Perangkat ini berada

di ITS, yang tergabung dalam domain ac (*academic*) dan seluruhnya berada pada domain id (Indonesia). Singkatnya, perangkat ns1 berada dalam its.ac.id. Jenis organisasi lain di Indonesia adalah go (lembaga pemerintah), co (lembaga komersial), dan org (selain di atas / organisasi swadaya masyarakat)

Top level domain yang digunakan pada Internet adalah singkatan nama geografis negara. Beberapa contoh lain untuk domain adalah:

- a. ca (Canada)
- b. fr (Perancis)
- c. jp (Jepang)
- d. nl (Belanda)
- e. th (Thailand)
- f. uk (Inggris)

Adapun top level domain berdasarkan organisasi, seperti contoh berikut:

- a. com organisasi komersial
- b. edu institusi pendidikan
- c. gov lembaga pemerintahan
- d. mil organisasi militer
- e. net organisasi yang mendukung network
- f. org organisasi lain yang tidak tergolong kelompok di atas

Manusia lebih mudah menggunakan dan mengingat nama, karena sifatnya yang informatif. Namun demikian, komunikasi komputer pada *TCP/IP* menghendaki nomor-nomor alamat IP sebagai alamat untuk proses mapping antara hostname dan alamat IP. Jika ingin berhubungan dengan komputer bernama mail.its.-sby.edu, maka komputer tempat kita berada harus mengetahui nomor alamat IP dari mail.its-sby.edu.

Langkah pertama yang dilakukan adalah melihat pada *file database* pada komputer itu sendiri. Jika pada *file database* lokal terdapat baris: mail.its-sby.edu IN A 167.205.169.82. Maka komputer dengan cepat mengetahui alamat IP yang akan dituju dan dari tabel *routing* dapat diketahui kemana paket harus dikirimkan.

Untuk memungkinkan suatu komputer dapat berhubungan dengan komputer dimanapun di Internet, sangat sulit dan tidak efisien bila seluruh

komputer memiliki seluruh daftar *hostname* yang ada didunia. Oleh karena itu, diberikan *host-host* yang memberikan layanan untuk *mapping hostname*. Perangkat seperti ini dikenal dengan sebutan *name server / domain name server*. Sesuai dengan namanya, wewenang suatu *name server* dapat dibag-bagi menurut *domain name* yang dibawahnya. Misalnya ada *name server* yang memegang *top level domain *.id*. Idealnya, *name server* ini memiliki daftar alamat IP dan *hostname* dari setiap komputer yang ada di Indonesia. Tetapi tentu saja ada keterbatasan untuk mengetahui alamat IP dan *hostname* dari perangkat-perangkat yang berada pada lingkungan instansi tertentu yang lebih kecil. Untuk data yang lebih spesifik, misalnya **.ac.id* atau **.its.ac.id*, *name server* ini dapat berhubungan dengan *name server* yang membawahi *domain* tersebut. [7]

2.2.6 Proxy

Proxy Server bertindak sebagai *gateway* terhadap dunia ini Internet untuk setiap komputer klien. *Proxy server* tidak terlihat oleh komputer klien: seorang pengguna yang berinteraksi dengan Internet melalui sebuah *proxy server* tidak akan mengetahui bahwa sebuah *proxy server* sedang menangani *request* yang dilakukannya. *Web server* yang menerima *request* dari *proxy server* akan menginterpretasikan *request-request* tersebut seolah-olah *request* itu datang secara langsung dari komputer klien, bukan dari *proxy server*. [8]

Proxy server memiliki 3 hal, yaitu *filtering*, *firewalling* dan *caching*. Pengertian dari ketiga hal tersebut adalah sebagai berikut: [8]

1. Filtering

Proxy server digunakan untuk membatasi akses *client*. Misal *client* tidak boleh membuka situ-situs yang sudah ditentukan untuk tidak dapat dibuka, seperti situs porno atau situs yang di dalamnya mengandung kekerasan dan unsur SARA. Selain itu dapat juga diatur dari jam berapa seorang dapat mengakses internet.

2. Firewalling

Proxy digunakan untuk koneksi internet. jaringan lokal dapat diatur agar jika *client* ingin menggunakan koneksi ke internet, *client* harus mengisi

proxy terlebih dahulu dan jika tidak *client* tidak dapat terhubung ke internet. *IP Address* dari *client* juga dapat di atur agar *IP address* mana saja yang dapat diperbolehkan mengakses *proxy server*.

3. *Caching*

Caching merupakan menyimpan *file* yang di akses *user* dari internet dan akan di gunakan lagi jika ada *user* yang mengakses *file* yang sama jadi dapat menghemat *bandwidth* yang di gunakan ke internet.

2.2.7 VPN (*Virtual Private Network*)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau *network* itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. [9]

2.2.7.1 Jenis-Jenis VPN

VPN telah dikembangkan menjadi beberapa jenis. Para ahli berbeda pendapat tentang pembagian jenis VPN tersebut. Ada yang membagi VPN berdasarkan cakupan area, yaitu Internet, Externet, dan Intranet. Ada yang membagi VPN berdasarkan jenis protokol yang digunakan. Secara umum VPN dapat dikelompokan menjadi: [10]

1. *Remota Access* VPN

Remota Access VPN disebut juga *Virtual Private Dial-Up Network* (VPDN). VPDN adalah jenis *user to LAN connection*. Artinya, *user* dapat melakukan koneksi ke *private network* dari manapun, apabila diperlukan.

2. *Site to Site* VPN

Site to Site VPN diimplementasikan dengan memanfaatkan perangkat *dedicated* yang dihubungkan via internet. *Site to Site* VPN digunakan untuk menghubungkan area yang sudah tetap.

2.2.7.2 Protokol VPN

Beberapa protokol yang ada di dalam VPN adalah sebagai berikut. [11]

1. PPTP (*Point-to-Point Tunneling Protocol*)

PPTP merupakan protokol jaringan yang dikembangkan oleh Microsoft dan Cisco yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi instansi dengan membuat sebuah VPN melalui *TCP/IP*. Teknologi jaringan yang terdapat pada PPTP adalah pengembangan dari *remote access Point-to-Point Protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP membungkus paket PPP menjadi IP *datagrams* agar dapat ditransmisikan melalui internet atau jaringan publik berbasis *TCP/IP*. PPTP juga dapat digunakan pada jaringan *private LAN-to-LAN*.

2. L2TP (*Layer 2 Tunneling Protocol*)

L2TP merupakan *tunneling protocol* yang memadukan dua buah *tunneling* protokol yaitu *Layer 2 Forwarding* milik Cisco dan PPTP yang dimiliki Microsoft. L2TP umumnya digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang dapat membawa semua jenis protokol komunikasi di dalamnya dan biasanya menggunakan port 1702 dengan protokol UDP. Terdapat dua model *tunnel* yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung *tunnel* berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*.

3. IPSec (IP security)

IPSec adalah pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya. Pada dasarnya paket IP tidak memiliki keamanan, sehingga tidak ada jaminan bahwa paket yang diterima sama dengan paket ketika ditransmisikan oleh si pengirim paket. Paket IP yang tidak memiliki keamanan atau *security*, sangat mudah untuk diketahui isinya dan alamat IP itu sendiri. IPSec adalah metode yang bertujuan untuk menjaga keamanan IP *datagram* ketika paket ditransmisikan pada *traffic*. Sehingga IPSec

menjadi suatu mekanisme yang diimplementasikan pada VPN. IPSec berada pada layer tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada atasnya. IPSec terdiri dari dua buah *security* protokol yaitu

- a. AH (*Authentication Header*) melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut.
- b. ESP (*Encapsulating Security Header*) melakukan enkripsi dan layanan autentifikasi.

Dua buah protokol tersebut dapat dikombinasikan atau berdiri sendiri dalam penyediaan keamanan. IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu AH dan ESP keduanya dapat dikombinasikan ataupun berdiri sendiri. Dengan menggunakan IPSec maka suatu sistem dapat memilih protokol *security* apa yang akan digunakan, dikarenakan IPsec berada pada level IP.

4. *Secure Sockets Layer* (SSL) VPN

SSL merupakan suatu standar teknologi keamanan untuk menjamin data yang melalui *webserver* dan *webbrowser* dengan membuat koneksi yang dienkripsi, antara *server* atau situs dengan pengunjungnya. Tanpa SSL data akan mudah dilihat dan dirubah saat dikirim melalui internet. SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server. Protokol SSL mengotentikasi *server* kepada client menggunakan kriptografi kunci publik dan sertifikat digital. Protokol ini juga menyediakan otentikasi *client* ke *server*. Algoritma kunci publik yang digunakan adalah RSA, dan untuk algoritma kunci rahasia yang digunakan adalah IDEA, DES, 3DES, AES.

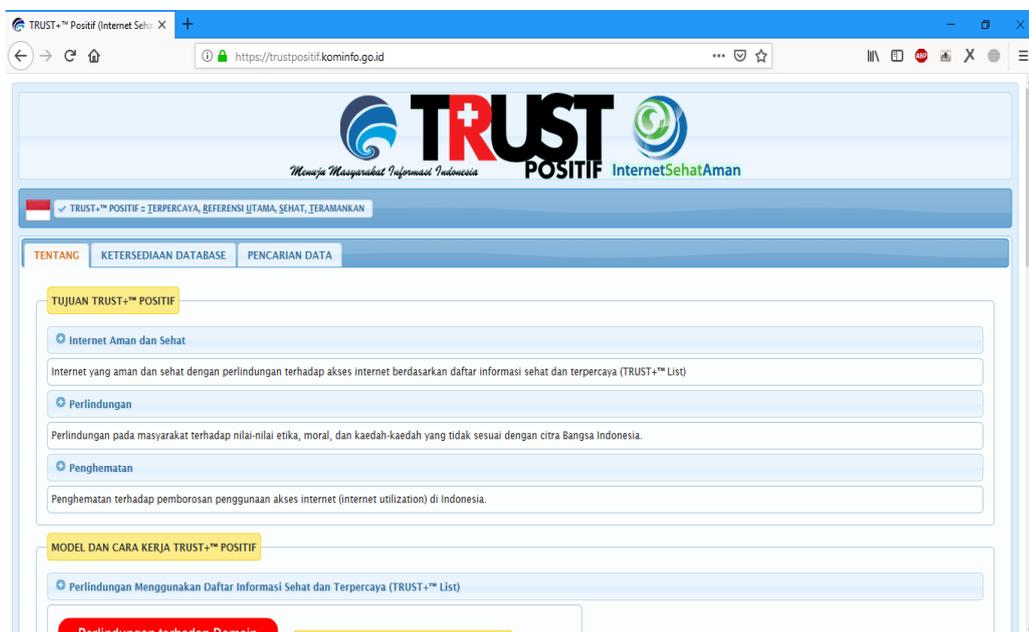
5. OpenVPN

OpenVPN adalah sebuah solusi VPN yang antar *platform* aman dan sangat mudah dikonfigurasi dengan menggunakan antar muka *virtual* yang disediakan oleh *driver* jaringan *universal TUN / TAP*.

2.2.8 Jenis Konten Negatif

Konten negatif kini begitu bertebaran di internet. Internet bukan hanya milik segelintir orang namun milik kita semua apa jadinya jika konten-konten negatif bertebaran di internet namun kita tidak bisa bertindak karena tidak memiliki kuasa. Konten negatif yang dimaksudkan didalam penelitian ini yaitu seperti pornografi, Judi online, aplikasi chat, hingga sosial media. Adapun list dari konten-konten negatif tersebut terdapat di *database* situs Trust+Positif kominfo yaitu:

<https://trustpositif.kominfo.go.id/>



Gambar 3.4 Situs Trust+Positif Kominfo

2.2.9 Penelitian Terdahulu

Penelitian ini dilakukan tidak terlepas dari hasil penelitian-penelitian terdahulu yang pernah dilakukan sebagai bahan perbandingan dan kajian. Adapun hasil-hasil penelitian yang dijadikan perbandingan tidak terlepas dari topik peneliti yaitu mengenai penerapan *transparent* DNS, pencegahan penggunaan proxy dan VPN menggunakan *firewall* dengan metode layer7 protocol mikrotik untuk optimalisasi *filtering* konten negatif.

Tabel 2.4 Penelitian Terdahulu

| Nama Peneliti | Judul Penelitian | Hasil Penelitian |
|--------------------------|--|---|
| Tengku Ahmad Riza (2015) | Implementasi Mikrotik <i>Proxy</i> Pada Jaringan RT/RW Di Komplek Pasirjati [13] | Untuk membangun jaringan di sebuah kompleks perlu peralatan yang digunakan komputer <i>server, client, LAN card, kabel dan konektor, repeater, bridge, router, gateway</i> dan modem. |
| Imam Riadi (2015) | <i>Block</i> Situs Dengan Mikrotik <i>Layer 7</i> Dan Web <i>Proxy</i> [6] | Banyaknya <i>user</i> yang mengakses situs terlarang, dan melakukan <i>browsing</i> dengan situs yang sama berulang kali sehingga diperlukan solusi untuk masalah ini. Salah satu metode untuk menangani masalah ini adalah dengan menggunakan VPN untuk kemudahan akses ke jaringan lokal dan pengguna <i>Proxy Server</i> sebagai <i>web caching</i> dan <i>web filtering</i> |
| Irsan Ramli (2016) | Implementasi <i>Firewall</i> Dengan Menggunakan Mikrotik [14] | Biasanya dilakukan dengan cara mendefinisikan IP <i>address</i> , baik itu <i>src-address</i> maupun <i>dst-address</i> . |
| Sumaryanto (2014) | Protokol Keamanan Berbasis <i>Proxy</i> dalam Jaringan Peralatan Bergerak [15] | Dalam sistem ini peralatan yang dipakai menggunakan <i>proxy software</i> yang dipercaya dapat bekerja pada peralatan <i>hardware</i> ataupun pada komputer |

| | | |
|----------------------|--|---|
| | | yang digunakan. Sistem keamanan dan privasi dijalankan dengan menggunakan dua buah protokol untuk komunikasi alat ke <i>proxy</i> yang aman, dan sebuah protokol untuk komunikasi <i>proxy-proxy</i> yang aman |
| Dian Novianto (2015) | Kajian Penggunaan Mikrotik Router Sebagai Router Pada Jaringan Komputer [16] | <i>Mikrotik Router</i> adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melakukan data melalui sebuah jaringan atau internet menuju sasarannya, melalui sebuah proses yang dikenal sebagai <i>routing</i> . |

