BAB 2

LANDASAN TEORI

Untuk merancang VPN diperlukan pengetahuan tentang jaringan komputer. VPN (Virtual Private Network) adalah termasuk jaringan komputer yang bersifat private atau pribadi (bukan untuk akses umum) yang menggunakan medium umum (misalnya internet) untuk menghubungkan antar remote-site secara aman. Walaupun menggunakan medium yang bersifat umum atau non-pribadi, sebuah jaringan VPN harus memiliki keamanan yang baik. Traffic antar remote-site tidak mudah untuk disabotase dan juga dapat mencegah seseorang menyusupkan traffic yang tidak semestinya ke dalam remote-site.

Untuk merancang sistem jaringan Virtual Private Network (VPN) perlu memahami sistem jaringan secara umum terlebih dahulu. Oleh karena itu, pada awal bab ini akan dijelaskan sistem jaringan secara umum termasuk layering OSI. Karena sistem jaringan VPN yang akan dirancang harus melalui jaringan internet, maka teori tentang internet, termasuk protocol TCP/IP juga dijelaskan pada bab ini.

Pada bab ini akan menjelaskan tentang teori-teori umum dan teori-teori khusus mengenai Virtual Private Network (VPN). Untuk itu pada teori umum akan menjelaskan mengenai definisi jaringan secara umum, topologi jaringan sampai pada kelas dan pengalamatan IP. Sementara pada teori khusus akan menjelaskan mengenai definisi umum dari Virtual Private Network (VPN), fungsi dari VPN, jenis VPN,

keamanan teknologi VPN, tunneling dan aplikasi VPN yang dipakai pada penulisan skripsi ini.

2.1 Teori Dasar/Umum

2.1.1 Definisi Jaringan Komputer

Jaringan Komputer adalah beberapa komputer yang saling berhubungan dapat melakukan komunikasi dan *share resources* antara satu dengan yang lainnya menggunakan perangkat keras jaringan, seperti *ethernet card*, *bridge*, *modem*, dan lain-lain (ANDI dan Wahana Komputer, 2005, p1). Pada dasarnya tujuan dari pembuatan suatu jaringan komputer adalah untuk :

a. Menghemat penggunaan hardware seperti CPU, *harddisk*, dan *printer* agar dapat dipakai secara bersama-sama tanpa terkendala lokasi / jarak dan juga dapat menekan biaya pembelian *hardware* dengan mengoptimalkan pemakaian sumber daya tersebut.

b. Mempermudah *sharing* data antara komputer satu dengan komputer yang lainnya.

c. Dapat melakukan pemindahan data (*transferring* data). Dan komunikasi antar komputer seperti *chatting*, *instant messanging*, *teleconference* dan *e-mail*.

d. Dapat mengakses informasi secara cepat dan mudah dengan *web browsing* melalui internet.

e. Terjaminnya keamanan data. Sistem jaringan komputer akan memberikan perlindungan terhadap data, jaminan keamanan tersebut diberikan melalui pemberian hak akses dan *password*.

2.1.2 Klasifikasi Jaringan Komputer

Terdapat 3 jenis klasifikasi jaringan komputer utama yang biasa digunakan sekarang ini yaitu:

1. Local Area Networking (LAN)

Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor perusahaan atau pabrik-pabrik untuk memakai bersama resource (misalnya, *printer*, *scanner*) dan saling bertukar informasi. Teknologi LAN yang saat ini banyak digunakan adalah *ethernet / fast ethernet, token ring,* FFID, dan *Wireless*-LAN. LAN pada dasarnya dirancang untuk kondisi berikut :

a. Kebutuhan dalam area geografis terbatas (kecil).
b. Memberikan akses kepada *user-user* terhadap media dengan *bandwidth* yang tinggi.
c. Melakukan koneksi antar *device* yang berdekatan.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) marupakan jaringan dalam sebuah kota dengan daerah operasi yang lebih luas dari LAN tetapi lebih kecil dari WAN. Jangkauan dari MAN ini antara 10 sampai 50 km, MAN merupakan jaringan yang tepat untuk membangun jaringan kantor-kantor yang letaknya berdekatan dalam sebuah kota dan dapat pula digunakan untuk keperluan pribadi atau umum. MAN mampu menunjang data, suara, dan bahkan dapat berhubungan dengan jaringan televisi kabel.

3. Wide Area Networking (WAN)

Wide Area Networking (WAN) merupakan jaringan yang jangkauannya mencakup area geografis yang luas, seringkali mencakup sebuah sebuah negara bahkan benua atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain. Tujuan dirancangnya jaringan WAN adalah untuk :

a. Berkomunikasi antar *user* lain yang berbeda negara dan benua secara *real time.*
b. Beroperasi dengan area geografis yang luas.

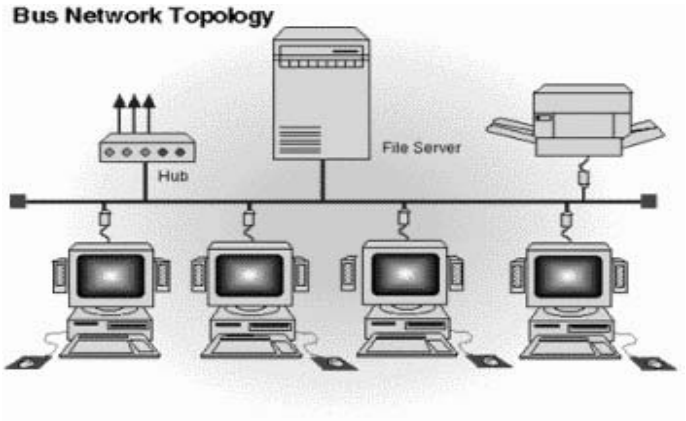
c. Dapat melakukan pengiriman *e-mail,* internet, *transfer file,* dan *e-commerce* dalam area geografis yang luas.

2.1.3 Topologi Jaringan

Topologi jaringan (LAN) adalah suatu cara (*logic*) untuk menghubungkan komputer satu dengan komputer lain sehingga membentuk suatu jaringan. Dan juga digunakan untuk menggambarkan bentuk fisik dalam sebuah jaringan komputer. Topologi jaringan yang biasa digunakan pada jaringan komputer adalah sebagai berikut :

1. **Topologi *Bus***

   Topologi *bus* menghubungkan beberapa *node*. Setiap *node* melakukan tugasnya masing-masing. Setiap komputer disambung dengan *T-Bus* dimana kedua ujungnya diberi sambungan resistor dengan nilai resistansi sebesar 50 *ohm* yang disebut dengan *terminator*. Nilai resistansi tersebut tergantung dari jenis media yang digunakan dalam topologi ini. Dan nilai 50 ohm tersebut merupakan nilai resistansi dari kabel koaksial, sedangkan untuk kabel fiber optic maka nilai resitansi tersebut akan berbeda. Metode access pada topologi ini adalah broadcast, yang mana data akan dikirimkan ke semua komputer/berbagai lokasi dan tidak memerlukan respon balik dari penerimanya.



Gambar 2.1 Topologi *Bus*

Kelebihan Topologi *Bus* :

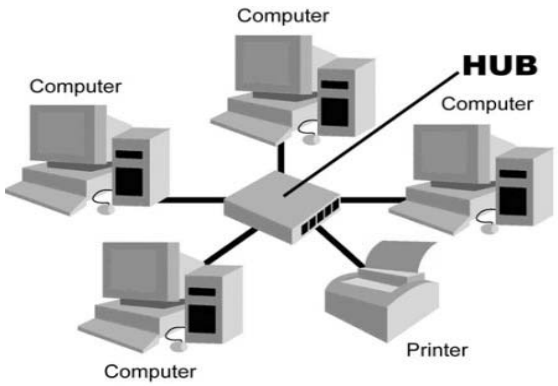
a. Murah karena tidak menggunakan banyak media dan mudah karena media yang digunakan banyak di pasaran.
b. Setiap komputer dapat saling berhubungan langsung.
c. Jika satu *node* rusak, tidak mengganggu *node* lain, karena setiap *node* terhubung melalui *bus*.

Kekurangan Topologi *Bus* :

a. Sering terjadi *hang* atau *crosstalk*, jika *user* menggunakan *bus* yang sama dan lebih dari satu pasang.
b. Tidak dapat digunakan secara bersamaan dalam waktu yang sama, sehingga harus bergantian dengan menambah *relay*.
c. Jika *bus* rusak, semua *node* tidak berfungsi sehingga kontrol manajemen data menjadi sulit.

2. Topologi *Star*

Topologi *Star* merupakan bentuk topologi jaringan yang berupa konvergensi dari *node* tengah ke setiap *node* sehingga pengguna komputer dapat berhubungan langsung ke *server* dan tidak perlu berhubungan ke pengguna komputer lain. Metode access pada topologi ini adalah broadcast, yang mana data akan dikirimkan ke semua komputer/berbagai lokasi dan tidak memerlukan respon balik dari penerimanya.



Gambar 2.2 Topologi *Star*

Kelebihan Topologi *Star* :

a. Akses *server* cepat dan tingkat keamanan tinggi.
b. Menampung banyak pengguna komputer yang melakukan banyak komunikasi ke *server*.
c. Kontrol manajemen lebih mudah karena bersifat terpusat.

Kekurangan Topologi *Star* :

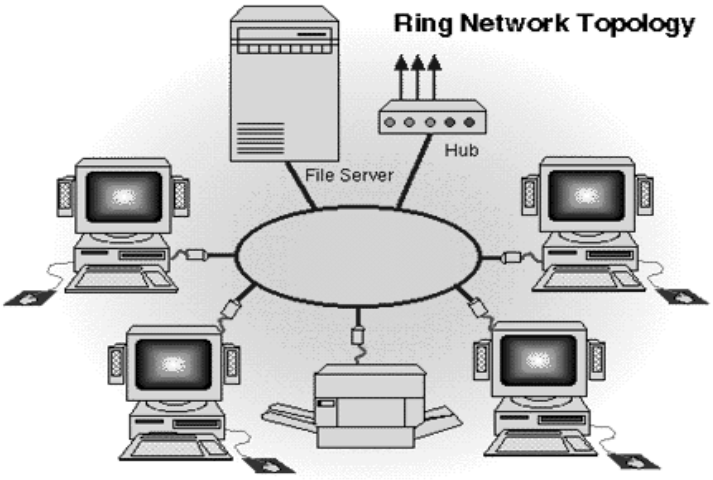
a. Jika dua pengguna ingin berkomunikasi, maka harus melalui *server* terlebih dahulu sehingga ada kemungkinan

terdapat kesalahan jika sambungan setiap pengguna *server* kurang baik.

b. Jika pusat *node* atau terminal rusak, maka semua sistem ikut rusak.

3. Topologi *Ring*

Topologi cincin adalah topologi jaringan dimana setiap titik terkoneksi ke dua titik lainnya, membentuk jalur melingkar membentuk loop tertutup. Pada topologi cincin, komunikasi data dapat terganggu jika satu titik mengalami gangguan. Jaringan FDDI mengantisipasi kelemahan ini dengan mengirim data searah jarum jam dan berlawanan dengan arah jarum jam secara bersamaan.



Gambar 2.3 Topologi *Ring*

Kelebihan Topologi *Ring* :

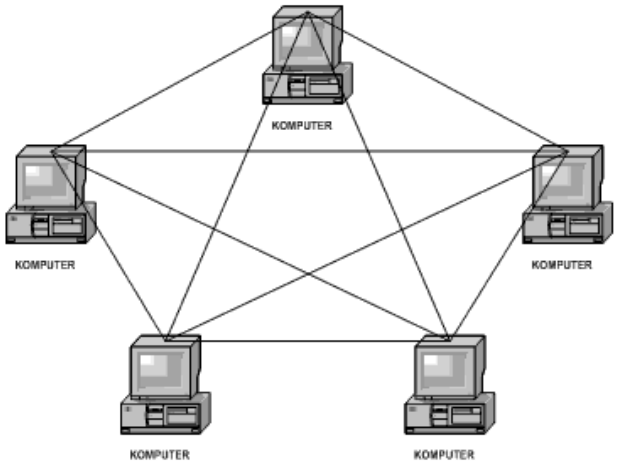
a. Tidak ada komputer yang memonopoli jaringan, karena setiap komputer mempunyai hak akses yang sama terhadap *token*.
b. Data mengalir *point to point* atau satu arah sehingga terjadinya kesalahan transmisi (*transmission error*) dan *collision* dapat dihindarkan.

Kekurangan Topologi *Ring* :

a. Data yang dikirim bila melalui banyak komputer maka akan menyebabkan transfer data menjadi lambat.

4. Topologi *Mesh*

Topologi *Mesh* memilki nama lain yaitu topologi *web*, topologi *switch*, topologi *plex*, atau topologi *fully connected*. Topologi ini merupakan bentuk jaringan dengan *node* yang saling berhubungan dengan *node* lain melalui beberapa link. Topologi ini menggunakan rumus umum = (n * (n - 1)) / 2 untuk menggunakan link. Pada rumus tersebut, n menunjukkan banyaknya node yang digunakan.



Gambar 2.4 Topologi *Mesh*

Kelebihan Topologi Mesh :

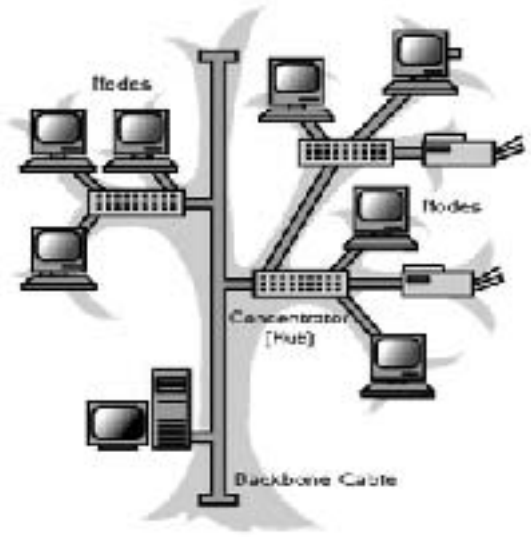
a. Memiliki sifat *Robust*, yaitu apabila terjadi gangguan pada koneksi komputer A dengan komputer B karena rusaknya kabel koneksi (*links*) antara A dan B, maka gangguan tersebut tidak akan mempengaruhi koneksi komputer A dengan komputer lainnya.
b. Mampu menampung banyak pengguna aktif serta *privacy* dan *security* pada topologi ini lebih terjamin.
c. Hubungan *dedicated links* menjamin data langsung dikirimkan ke komputer tujuan tanpa harus melalui komputer lainnya sehingga dapat lebih cepat.

Kekurangan Topologi Mesh :

a. Membutuhkan banyak kabel dan *port* I/O, semakin banyak komputer di dalam topologi mesh maka diperlukan semakin banyak kabel *links* dan *port* I/O.
b. Hal tersebut sekaligus juga mengindikasikan bahwa topologi jenis ini membutuhkan biaya yang relatif mahal.

5. Topologi Tree

Topologi ini seperti membentuk sebuah pohon dengan cabangnya. Topologi ini terdiri atas *central node* (komputer spesifikasi tinggi) dan *node* (komputer spesifikasi rendah) yang saling berhubungan secara berjenjang. *Central node* sebagai *host* komputer merupakan jenjang tertinggi (*top hierarchical*) yang berfungsi untuk mengkoordinasi node pada jenjang dibawahnya. Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin keatas mempunyai hirarki semakin tinggi.



Gambar 2.5 Topologi *Tree*

Kelebihan Topologi Tree :

a. Kontrol manajemen lebih mudah karena bersifat terpusat dan terbagi dalam tingkatan atau jenjang.
b. Lebih mampu menjangkau jarak yang lebih jauh dengan mengaktifkan fungsi *repeater* yang dimiliki oleh *hub*.

Kelemahan Topologi Tree :

a. Jika salah satu *node* rusak, maka *node* yang berada di jenjang bagian bawah tidak berfungsi.
b. Kabel yang digunakan menjadi lebih banyak sehingga diperlukan perencanaan yang matang dalam pengaturannya, termasuk di dalamnya adalah tata letak ruangan.

2.1.4 Protokol Jaringan

Protokol jaringan merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer lain. Aturan-aturan ini meliputi tata cara bagaimana agar komputer bisa saling berkomunikasi.

Kunci pokok suatu protokol adalah :

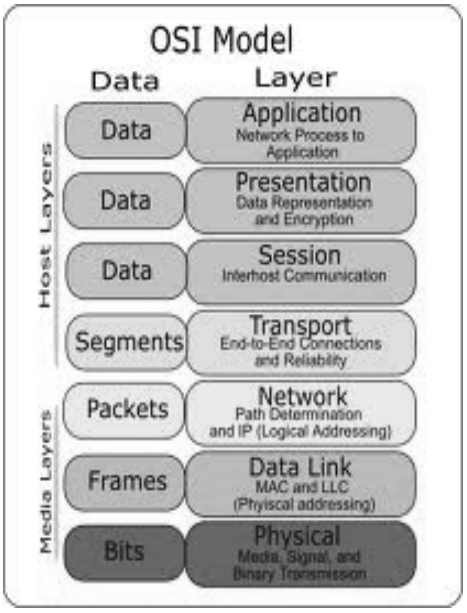
- Syntax, merupakan format data dan cara pengkodean yang digunakan untuk mengkodekan sinyal.
- Semantics, digunakan untuk mengetahui maksud dari informasi yang dikirim dan mengoreksi kesalahan yang terjadi dari informasi tadi.
- Timing, digunakan untuk mengetahui kecepatan transmisi data.

Model umum yang dijadikan referensi untuk mempelajari protokol jaringan dan juga sabagai dasar bagi pengembangan standar-standar komunikasi yaitu model referensi Lapisan *Open System Interconnection* (OSI Layer) dan model referensi TCP/IP yang mana merupakan protokol jaringan yang sangat umum digunakan untuk *internetworking*.

2.1.4.1 Model OSI Layer

Model *Open System Interconnection* (OSI) dikembangkan oleh *Internasional Standard Organization* sebagai model arsitektur jaringan untuk merancang komunikasi dan sebagai kerangka dasar untuk mengembangkan protokol lainnya. Model

referensi OSI dapat menampilkan fungsi-fungsi dan cara kerja jaringan yang terjadi pada setiap lapisannya dan juga dapat memvisualisasi bagaimana informasi atau paket-paket data disampaikan dari program-program aplikasi melalui media jaringan ke program aplikasi lainnya yang berlokasi di komputer lain, bahkan meski pengirim dan penerima berada dalam tipe *network* yang berbeda. Dalam model referensi OSI terdapat tujuh buah layer komunikasi. Masing-masing layer mengilustrasikan fungsi-fungsi khusus dan batasan-batasan fungsi ini disebut dengan layering. Setiap layer mempunyai properti yang menggunakan fungsi layer di bawahnya, memproses data pada layer tersebut, lalu mengirim pada layer selanjutnya.



Gambar 2.6 Model OSI Layer

1. Layer 1 – *Physical layer*

Physical layer merupakan lapisan terbawah pada model OSI dan berhubungan langsung dengan *hardware*. Lapisan ini menetapkan spesifikasi-spesifikasi *fungsional, electrical, mechanical*, dan *procedural* untuk aktivasi, perawatan dan deaktivasi link *physical* di antara sistem-sistem tujuan. Lapisan ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronasi *bit*, arsitektur jaringan, topologi jaringan dan pengkabelan. Selain itu, juga mendefiniskan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan kabel atau radio. Peralatan yang bekerja pada *physical layer* antara lain repeater, *network card* dan hub.

2. Layer 2 – Data link layer

Data link layer berfungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format, yang disebut sebagai *frame*. Selain itu pada layer ini juga dilakukan *error checking* menggunakan CRC (Cyclic Redudancy Checking), *flow control*, pengalamatan perangkat keras (seperti halnya MAC Address), dan menentukan bagaimana perangkat-perangkat jaringan seperti *hub*, *bridge*, *repeater*, dan *switch layer 2* beroperasi. Data link layer dibagi kembali menjadi 2 jenis yaitu lapisan *Logical Link Control* (LLC) dan *Media*

Access Contol (MAC). Peralatan yang bekerja pada layer ini adalah *switch* dan *bridge*.

3. Layer 3 – Network layer

Network layer bertanggung jawab untuk menangani perpindahan paket-paket data antara dua peralatan yang terhubung secara kompleks dan menentukan protokol untuk meneruskan data agar dapat memastikan bahwa informasi tiba di tujuan yang benar. Layer ini juga berfungsi mendefinisikan alamat-alamat IP (*addressing*), membuat *header* untuk paket-paket, layanan *gateway* dan kemudian melakukan routing melalui *internetworking* dengan menggunakan *router* dan *switch layer-3*.

4. Layer 4 – Transport layer

Layer ini memastikan data yang dikirim bebas dari kesalahan, urutannya benar, dan tidak ada data yang hilang atau terduplikasi. Layer ini berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi (komputer) tujuan setelah diterima. Selain itu, pada layer ini juga membuat sebuah tanda bahwa paket diterima dengan sukses *(acknowledgment*/ACK) dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

5. Layer 5 – Session layer

Session layer betanggung jawab untuk membangun, mengelola, dan mengakhiri sesi-sesi di antara dua *host* yang berkomunikasi. *Session layer* memberikan layanan-layanannya ke presentation layer. Dan juga mensinkronisasi percakapan di antara dua *host* dan mengatur pertukaran datanya. Selain pengaturan sesi-sesi, *session layer* menyajikan aturan-aturan untuk efisiensi transfer data, kelas layanan, dan pengecualian pelaporan atas permasalahan-permasalahan *session layer*, *presentation layer*, dan *application layer*.

6. Layer 6 – Presentation layer

Layer ini berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan agar dapat dimengerti oleh aplikasi di sistem lain. Selain itu jika diperlukan, lapisan ini juga dapat menerjemahkan beberapa data format yang berbeda, kompresi dan enkripsi. Jadi yang terjadi di presentation layer adalah manipulasi data, bukan fungsi komunikasi.

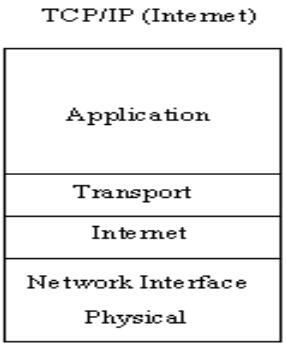
7. Layer 7 – Application layer

Application layer merupakan layer teratas dari model OSI layer. Layer ini adalah layer yang paling dekat dengan pengguna (*user*) dimana *user* dapat berinteraksi secara langsung dengan komputer. Layer ini bertanggung jawab untuk mengidentifikasi dan membangun ketersediaan komunikasi yang diinginkan serta menyediakan pelayanan distribusi informasi. Selain itu layer ini juga 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, dan NFS.

2.1.4.2 Model referensi TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (software) di sistem operasi. Istilah yang diberikan kepada

perangkat lunak ini adalah TCP/IP stack. Model referensi TCP/IP mempunyai 4 layer, yaitu : *application layer*, *transport layer*, *internet layer, network access layer*.



Gambar 2.7 Model Referensi TCP/IP

1. Network access layer

Network access layer merupakan gabungan antara *physical layer* dan *data link layer* pada OSI layer. Layer ini berfungsi mengatur pertukaran data antara *end system* dengan jaringan yang terhubung dengannya dan meletakkan *frame-frame* data diatas media jaringan. 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* modem yang berjalan di atas *Public Switched Telephone Network* (PSTN), *Integrated Services Digital Network* (ISDN), serta *Asynchronous Transfer Mode* (ATM).

2. Internet Layer

Internet layer memiliki tugas untuk memilih rute terbaik yang akan dilewati oleh sebuah paket data dalam sebuah jaringan. Selain itu, layer ini juga bertugas untuk melakukan packet switching untuk mendukung tugas utama tersebut. Protokol-protokol yang berfungsi pada layer ini adalah *Internet Protokol* (IP), *Internet Control Message Protocol* (ICMP), *Internet Group Management Protocol* (IGMP), *Bootstrap Protocol* (BOOTP), *Address Resolution Protocol* (ARP), *Reverse Address Resolution Protocol* (RARP).

3. Transport layer

Transport layer menyediakan layanan pengiriman dari sumber data menuju ke tujuan data dengan cara membuat *logical connection* antara keduanya. Layer ini bertugas untuk memecah data dan menggabungkan kembali data yang diterima dari *application layer* ke dalam aliran data yang sama antara sumber dan pengirim data. *Transport layer* terdiri dari dua protokol yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP).

No.	TCP	UDP
1.	*Connection-Oriented*, sebelum data ditransmisikan terlebih dahulu dilakukan negoisasi untuk membuat sesi koneksi.	*Connectionless*, pesan yang dikirimkan tidak perlu melakukan negoisasi untuk membuat sesi koneksi.
2.	*Reassembly*, data diurutkan kembali di tujuan.	Data langsung dikirimkan ke *upper layer* begitu data sampai.
3.	*Reliable*, data yang dikirimkan memiliki nomor urut paket dan akan mendapatkan *acknowledgment* dari penerima, jika tidak akan ditransmisikan ulang	*Unreliable*, data dikirimkan sebagai datagram tanpa memiliki nomor urut dan mendapatkan *acknowledgment*
4.	*Flow control*, untuk mencegah data terlalu banyak dikirimkan pada satu waktu	Tidak terdapat *flow control*

Tabel 2.1 Perbedaan TCP dan UDP

4. Application layer

Application layer berfungsi untuk menangani high-level protocol, masalah representasi data, proses encoding, dan dialog control yang memungkinkan terjadinya komunikasi antar aplikasi jaringan.

Application layer berisi spesifikasi protokol-protokol khusus yang menangani aplikasi umum, diantaranya adalah :

- *HyperText Transfer Protocol* (HTTP) merupakan protokol yang dipakai untuk mayoritas komunikasi *World Wide Web* (WWW).
- *Simple Mail Transfer Protocol* (SMTP) merupakan suatu protokol yang dipakai *server mail* untuk mentransfer *e-mail.*
- *Telnet* merupakan suatu protokol yang dapat dipakai untuk me-*logon* ke *host* jaringan yang jauh. *Telnet* menawarkan para pemakai suatu kapabilitas dalam mengoperasikan program-program secara jauh dan memudahkan administrasi yang jauh. Telnet disediakan untuk semua sistem operasi dan mengurangi integrasi dalam lingkungan jaringan yang heterogen.
- *Simple Network Management Protocol* (SNMP) memungkinkan untuk mengelola node jaringan seperti *server, workstation, router, bridge*, dan *hub* dari host sentral. SNMP dapat dipakai untuk mengkonfigurasi *device* yang jauh, memantau kinerja jaringan, mendeteksi kesalahan jaringan, dan mengecek pemakaian jaringan.
- *Domain Name System* (DNS) merupakan seperangkat protokol dan layanan pada suatu jaringan TCP/IP, yang membolehkan para pemakai jaringan untuk mempergunakan nama-nama hirarki yang sudah dikenal ketika meletakkan *host* daripada harus mengingat dan memakai alamat IP-nya.

2.1.5 Pengalamatan IP

Alamat IP adalah deretan angka biner antar 32-*bit* sampai 128-*bit* yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Panjang dari angka ini adalah 32-*bit* (untuk IPv4 atau IP versi 4), dan 128-*bit* (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP.

2.1.5.1 Kelas-kelas IP

IP address dibedakan menjadi 5 kelas, yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Tujuan membedakan kelas IP adalah untuk menentukan jumlah komputer yang bisa terhubung dalam sebuah jaringan.

- **Kelas A**

  IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. *Bit* pertama dari IP address kelas A selalu di set 0 (nol) sehingga *byte* terdepan dari IP address kelas A selalu bernilai antara angka 0-127. Pada kelas ini, *network ID* adalah 8 *bit* pertama sedangkan untuk *host ID* adalah 24 *bit* berikutnya. IP address kelas A ini dapat menampung lebih kurang 16 juta *host* dan range IPnya adalah 1.xxx.xxx.xxx – 126.xxx.xxx.xxx.

- **Kelas B**

  IP address kelas B ini biasanya digunakan untuk jaringan yang berukuran sedang dan besar. Pada IP address kelas B ini 2 (dua) *bit* pertama dari IP selalu di set dengan 10 (satu nol) sehingga *byte* terdepan dari IP *address* kelas ini selalu bernilai 128-191. Pada IP *address* kelas B ini, *network ID* adalah 16 *bit* pertama sedangkan untuk *host ID* adalah 16 berikutnya. IP address kelas B ini dapat menampung lebih kurang 65.000 dan range IPnya adalah 128.0.xxx.xxx – 191.255.xxx.xxx.

- **Kelas C**

  IP address kelas C digunakan untuk jaringan yang lebih kecil seperti LAN. Pada IP address kelas C ini 3 (tiga) *bit* pertamanya selalu berisi 110 (satu satu nol). Bersama 21 *bit* berikutnya, angka ini membentuk *network ID* sebesar 24 *bit* dan 8 *bit* terakhir untuk *host ID*. IP address kelas C ini dapat menampung lebih kurang 2 juta network dengan masing-masing network memiliki 256 IP *address* dan range IPnya adalah 192.0.0.xxx – 223.255.255.xxx.

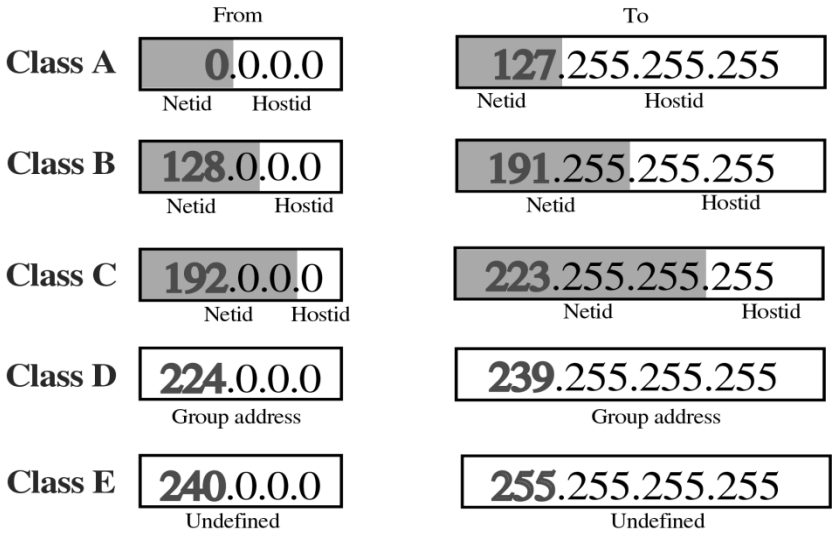
- **Kelas D**

  Kelas D merupakan kelas yang tidak dapat dipakai oleh publik karena satu blok kelas ini khusus dipakai untuk keperluan

multicast. Multicast adalah jenis transmisi layaknya broadcast, namu dalam skala yang lebih kecil dan dapat ditentukan.

- **Kelas E**

Kelas E merupakan kelas IP yang tidak digunakan dan khusus disimpan dengan tujuan sebagai cadangan untuk keperluan di masa mendatang.



Gambar 2.8 *Range* Alamat IP Tiap Kelas

2.1.5.2 Public dan Private IP *Address*

Selain itu IP *address* juga dibagi menjadi dua macam berdasarkan pemakaiannya di internet :

- Private IP *address*

Private IP *address* adalah alamat IP yang digunakan oleh sebuah komunitas, baik itu rumah ataupun sebuah perusahaan, untuk berkomunikasi antara komputer yang satu dengan yang lainnya dalam jaringan internal dan biasanya digunakan pada jaringan LAN.

***Private IP Address* Class**	***Private IP Address Range***
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0-172.31.255.255
C	192.168.0.0-192.168.255.255

Tabel 2.2 Pembagian *class pada private IP*

- Public IP *address*

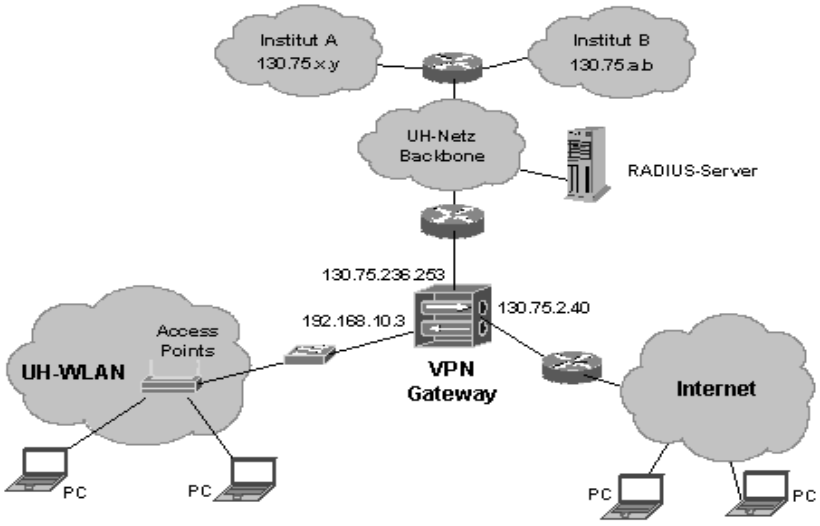
Public IP *address* adalah alamat IP yang digunakan untuk berkomunikasi antar komputer yang tersambung langsung dengan jaringan internet. Jenis IP ini digunakan oleh *Internet Service Provider* (ISP) dan lembaga-lembaga dunia yang mengatur lalu lintas internet. Range alamat yang dimiliki *Public* IP *Public* adalah semua alamat IP selain yang berada dalam *range private* IP dan IP *loopback*.

2.2 Teori Khusus

Pada bagian ini akan dijelaskan mengenai teori khusus yang dipergunakan dalam penelitian, yakni pengertian *virtual private network* (VPN), cara kerja VPN, fungsi dan kegunaan VPN, jenis-jenis VPN, dan macam-macam tunneling. Serta dijelaskan pula tentang aplikasi yang dipakai yakni OpenVPN dan Zentyal sebagai gateway dari VPN ini.

2.2.1 Pengertian *Virtual Private Network* (VPN)

Menurut K. V. Kale (2008, p69), *Virtual Private Network* (VPN) adalah jaringan *private* yang menggunakan jaringan publik seperti internet untuk menghubungkan *remote access* dan *user* secara bersama-sama dengan memberikan tingkat level privasi, *security*, *Quality of Service* (QoS), dan pengelolaan dimana jaringan tersebut dibangun seluruhnya dalam fasilitas yang dimiliki secara pribadi dan *dedicated*.



Gambar 2.9 : *Virtual Private Network*

2.2.2 Fungsi VPN

Teknologi VPN menyediakan tiga fungsi utama dalam penggunaannya. Fungsi utama tersebut adalah sebagai berikut :

1. **Kerahasiaan**

   Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang melewatinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan data menjadi lebih terjaga. Meskipun masih ada pihak yang dapat menyadap data, namun belum tentu pihak tersebut dapat membaca data itu dengan mudah karena data tersebut telah dienkripsi. Dengan menerapkan sistem enkripsi ini, maka tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

2. **Integritas data**

   Ketika melewati jaringan internet, data sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isi data tersebut, baik itu hilang, rusak, atau bahkan dimanipulasi isinya oleh orang lain. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuan tanpa cacat, hilang rusak, ataupun dimanipulasi oleh orang lain.

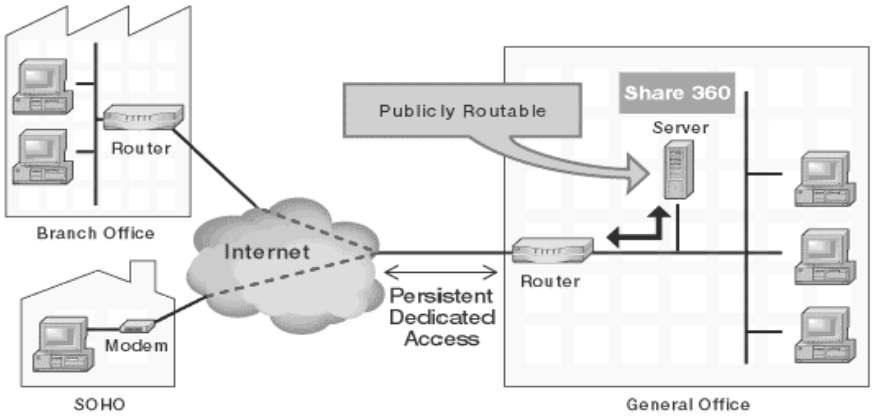
3. Autentikasi Sumber

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi *source* datanya. Kemudian alamat *source* data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

2.2.3 Jenis-jenis VPN

- **Remote Access VPN**

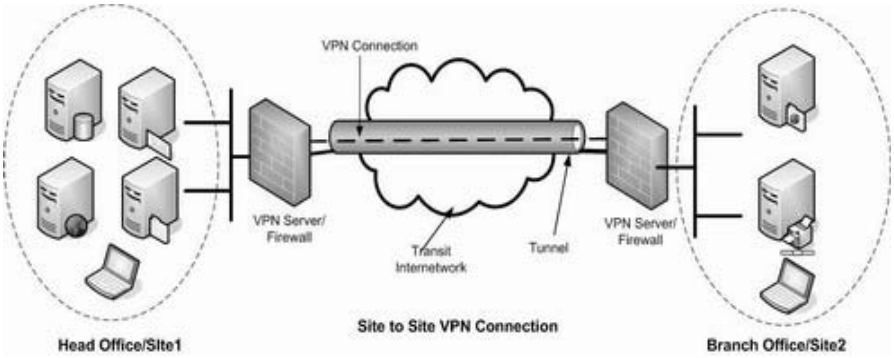
  Tipe VPN ini memungkinkan koneksi jarak jauh (remote access) bagi pegawai yang sedang bertugas di luar kantor, luar kota ataupun sedang di luar negeri untuk dapat akses ke LAN di kantor pusat menggunakan jaringan internet. Hal ini terutama sangat berguna untuk dapat menerima email yang tersedia di LAN kantor pusat. Selain itu, hal tersebut juga berlaku bagi kantor cabang yang tidak memiliki koneksi secara terus-menerus ke kantor pusat. Kantor cabang tersebut dapat melakukan koneksi *dial-up* lokal ke suatu ISP dan setelah itu melakukan koneksi ke kantor pusat.



Gambar 2.10 Remote Access VPN

- **Site-to-Site VPN**

  Site-to-Site VPN memungkinkan suatu *private network* diperluas melintasi jaringan internet atau layanan *public network* lainnya dengan cara yang aman. Site-to-Site VPN kadang disebut juga sebagai LAN-to-LAN VPN. Site-to-Site VPN merupakan suatu alternatif dari infrastruktur WAN yang biasa menghubungkan kantor-kantor cabang, kantor pusat, atau partner bisnis ke seluruh jaringan yang terdapat di perusahaan.



Gambar 2.11 Site-to-Ste VPN

Site-to-Site VPN dibedakan menjadi dua jenis, yaitu :

- **Intranet VPN**

  Intranet VPN digunakan untuk menghubungkan antara kantor pusat dengan kantor cabang atau kantor yang letaknya berjauhan melalui suatu *public infrastructure*.

- **Extranet VPN**

  Extranet VPN merupakan intranet dari suatu perusahaan yang diperluas untuk menggabungkan para pemakai dari luar perusahaan, seperti : pemasok, penjual, pelanggan dan relasi bisnis. Sehingga antara kedua perusahaan dapat saling bertukar dan berbagi informasi dengan cepat dan mudah dengan penambahan *firewall* untuk keamanan *internal network* .

2.2.4 Keamanan VPN

Seperti yang telah dijelaskan bahwa VPN menggunakan internet sebagai media perantaranya, maka keamanan pada jaringan VPN sangatlah diperlukan agar data yang dikirim dan diterima dapat terjamin keamanannya. Beberapa tipe keamanan yang dapat diterapkan pada teknologi VPN adalah enkripsi, autentikasi, autorisasi, dan firewall.

2.2.4.1 Enkripsi

Enkripsi merupakan salah satu cara yang digunakan untuk mengubah data asli (sebenarnya) menjadi bentuk sandi (*chipper text*) yang mana sandi-sandi tersebut hanya dapat dimengerti oleh pihak pengirim dan penerima data sehingga data tersebut tidak dapat dibaca oleh orang luar yang tidak mempunyai hak akses untuk melihat data tersebut. Untuk mengubah sandi (*chipper text*) tersebut ke bentuk semula maka digunakan teknik yang dinamakan *dekripsi*. Terdapat dua cara untuk melakukan proses enkripsi, yaitu enkripsi kunci simetrik dan enkripsi kunci asimetrik.

2.2.4.1.1 Enkripsi Kunci Simetrik

Pada enkripsi menggunakan kunci simetrik, setiap komputer memiliki kunci rahasia (kode) yang dapat digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan kunci yang digunakan untuk mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki oleh kedua komputer sehingga harus tercapai kesepakatan antara penerima dengan pengirim, misal dengan media telepon, email, atau bertemu langsung.

Metode enkripsi ini harus dijaga ketat agar tidak ada pihak luar yang mengetahuinya dan dengan mudah membaca data tersebut.

2.2.4.1.2 Enkripsi Kunci Asimetrik

Pada enkripsi kunci asimetrik, proses enkripsi dan dekripsi masing-masing menggunakan dua buah kunci yang berbeda, yaitu *private key* dan *public key* yang saling berhubungan secara sistematis. Private key dibuat oleh penerima pesan dan hanya penerima pesan tersebut yang dapat mengetahui isinya, dari private key inilah, sebuah public key terbentuk. Setelah public key terbentuk, public key tersebut dikirimkan kepada pihak yang ingin mengirimkan pesan. Oleh pengirim pesan, public key tersebut digunakan untuk mengenkripsi pesan yang akan dikirim. Setelah pesan tersebut di terima, maka penerima pesan tersebut harus menggunakan private key untuk mendekripsi pesan tersebut. Dikarenakan mempunyai cara kerja yang rumit dan tingkat keamanan yang lebih baik, maka banyak orang yang lebih menggunakan sistem pengenkripsian data seperti ini.

2.2.4.2 Autentikasi

Autentikasi merupakan salah satu proses untuk mengindetifikasi pengguna sehingga data yang dikirim akan menjadi jelas isi dan siapa pengirimnya. Biasanya dalam proses autentikasi, diperlukan *username* dan *password* sebagai alat verifikasinya. *Username* dan *password* ini dimaksudkan agar tidak sembarang orang dapat mengakses, mengirim ataupun mengambil data yang bersifat *private*.

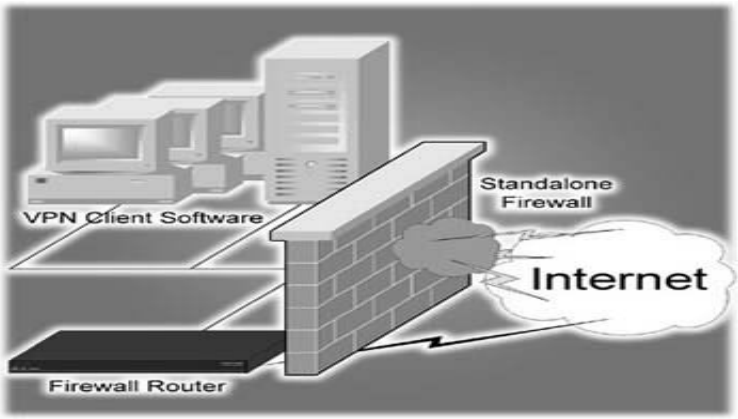
2.2.4.3 Autorisasi

Autorisasi adalah pencarian apakah orang yang sudah diidentifikasi (diautentikasi), diizinkan untuk memanipulasi sumber daya atau data tertentu di jaringan VPN tersebut. Proses autorisasi inilah yang menentukan apakah pengguna tersebut dapat melakukan perintah atau tugas yang dikehendakinya pada jaringan VPN tersebut.

2.2.4.4 Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software maupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring,

mambatasi, atau bahkan menolak suatu atau semua hubungan / kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, dan *local area network* (LAN). Firewall merupakan sebuah perangkat yang diletakkan antara *internet* dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan utama dari firewall adalah untuk menjaga agar orang yang tidak berwenang tidak dapat melakukan akses, baik ke dalam maupun keluar.



Gambar 2.12 *Firewall*

Firewall memiliki prinsip kerja dalam menjalankan kendalinya, prinsip kerja yang digunakan adalah sebagai berikut :

1. *Service Control* (Kendali Terhadap Layanan)

   Prinsip kerja berdasarkan tipe-tipe layanan yang digunakan di internet dan boleh diakses baik untuk ke

dalam ataupun keluar firewall. Firewall akan mengecek nomor IP address dan nomor port yang digunakan, baik pada protokol TCP dan UDP. Firewall bisa dilengkapi software proxy untuk menerima dan menterjemahkan setiap permintaan atas suatu layanan sebelum mengizinkannya. Selain itu, server juga bisa menggunakan software, misalnya untuk layanan web atau mail.

2. *Direction Control* (Kendali Terhadap Arah)

   Prinsip kerja berdasarkan arah dari berbagai permintaan (request) terhadap layanan. Layanan akan dikenali dan diizinkan melewati firewall.

3. *User Control* (Kendali Terhadap Pengguna)

   Prinsip kerja berdasarkan pengguna / *user* untuk dapat menjalankan suatu layanan. Dengan demikian, ada user yang dapat menjalankan suatu *service* dan ada yang tidak. User tidak dapat menjalankan *service* karena tidak diizinkan untuk melewati *firewall*. Prinsip ini biasa digunakan untuk membatasi akses keluar user jaringan lokal, namun bisa juga diterapkan untuk membatasi akses terhadap pengguna dari luar.

4. *Behavior Control* (Kendali Terhadap Perlakuan)

   Prinsip kerja berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, firewall dapat memfilter email untuk menanggulangi atau mencegah spam.

2.2.5 Tunneling

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP *Addressing* dan IP *Routing* yang sudah baik atau telah terhubung sehingga antara sumber *tunnel* dengan tujuan *tunnel* dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari *tunnel* tidak dapat berjalan dengan baik, maka *tunnel* tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun. Setelah *tunnel* tersebut terbentuk, maka koneksi *point-to-point* tersebut dapat langsung digunakan untuk mengirim dan menerima data. Dalam penerapannya di VPN, t*unnel* dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati *tunnel* tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi aman dan bersifat pribadi.

2.2.5.1 *Point to Point Tunneling Protocol* (PPTP)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP.

Teknologi jaringan PPTP merupakan pengembangan dari *remote access* Point-*to*-Point protocol yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan *private* LAN-*to*-LAN.

Umumnya terdapat tiga komputer yang diperlukan untuk membangun PPTP, yaitu sebagai berikut :

- Klien PPTP
- Network access server (NAS)
- Server PPTP

Akan tetapi tidak diperlukan network access server dalam membuat PPTP tunnel saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubung dengan server PPTP yang terhubung pada LAN yang sama.

2.2.5.2 *Layer 2 Tunneling Protocol* (L2TP)

L2TP adalah tunneling protokol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft. L2TP biasa digunakan dalam membuat *Virtual Private Dial Network* (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi di dalamnya. Paket data L2TP dikirim melalui protokol UDP. Terdapat dua model tipe L2TP yaitu :

- *Voluntary Tunnel*

  Voluntary Tunnel merupakan *tunnel* yang dibuat berdasarkan permintaan klien. Pada awalnya klien akan melakukan koneksi kepada ISP yang menyediakan jasa VPN. Setelah menerima permintaan klien, ISP tersebut membuatkan jalur khusus yang menghubungkan klien tersebut dengan VPN servernya.

- *Compulsory Tunnel*

  Berbeda halnya dengan *voluntary tunnel*, *compulsory tunnel* dibuat oleh perangkat *intermediate*. Perangkat *intermediate* ini bisa berupa dial-up server ataupun alat lainnya. Ketika klien dan *remote client* yang terhubung dengan LAN ingin membangun koneksi, mereka harus terhubung terlebih dahulu dengan perangkat *intermediate* yang biasanya terletak di ISP. Setelah

koneksi sudah terbuat maka perangkat inilah yang membuat tunnel.

2.2.5.3 IP *Security* (IPSec)

Ipsec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. Protokol yang berjalan dibelakang IPSec adalah:

1. AH (Authentication Header), menyediakan layanan *authentication* (menyatakan bahwa data yang dikirim berasal dari pengirim yang benar), *intregrity* (keaslian data), dan *replay protection* (transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengizinkan), juga melakukan pengamanan terhadap IP header (*header compression*).
2. ESP (*Encapsulated Security Payload*), menyediakan layanan *authentication*, *intregity*, *replay protection*, dan *confidentiality* (keamanan terjaga) terhadap data. ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah header.

2.2.6 Zentyal

Zentyal atau dengan nama sebelumnya *eBox* merupakan aplikasi *open source* untuk server jaringan terpadu yang menawarkan administrasi jaringan komputer mudah dan efisien untuk usaha kecil dan menengah. Zentyal dapat berfungsi sebagai gateway, *manager* infrastruktur, *unified threat manager*, *server* kantor, *server* komunikasi terpadu atau kombinasi dari fungsi di atas. *Source code* Zentyal dimiliki di bawah ketentuan GNU General Public License, serta dibawah ketentuan hak milik yaitu eBox Technology S.L. Keunggulan salah satunya adalah tampilannya yang *user friendly* karena memiliki *graphic user interface* (GUI) sehingga mudah digunakan dan dipelajari oleh user yang baru pertama kali menggunakan.

2.2.7 OpenVPN

OpenVPN adalah aplikasi open source yang mengimplementasikan teknik *Virtual Private Network* (VPN) untuk membuat koneksi *point-to-point* atau *site-to-site* dan fasilitas *remote access* secara aman. Untuk melakukan *autentifikasi* pada saat membangun suatu koneksi, OpenVPN menggunakan *pre-shared key*, *certificate*, dan *username / password*, yang mana untuk proses enkripsinya menggunakan OpenSSL

2.2.7.1 Kelebihan dan Kekurangan OpenVPN

OpenVPN menawarkan berbagai kelebihan diantaranya adalah :

- Layer 2 dan layer 3 VPN : OpenVPN menawarkan 2 mode dasar yang bekerja baik pada layer 2 maupun layer 3 VPN. Tunnel OpenVPN juga dapat mengirim ethernet frames, paket IPX, dan paket Windows Networking Browsing (NETBIOS).
- Konfigurasi proxy dan pendukungnya: OpenVPN mempunyai proxy pendukung dan dapat di konfigurasikan untuk bekerja sebagai TCP atau UDP, dan sebagai server atau client. Sebagai server, OpenVPN menunggu hingga client meminta koneksi. Dan sebagai client, OpenVPN mencoba untuk membangun sebuah koneksi berikut konfigurasinya.
- Fleksibilitas yang tinggi memungkinkan untuk melakukan *scripting* : OpenVPN menawarkan *scripting* individual. Script ini dapat digunakan untuk berbagai macam tujuan seperti *autentifikasi* untuk failover dan lainnya.
- Instalasi yang mudah pada setiap platform : Langkah instalasi serta penggunaan yang sangat mudah untuk dipelajari.

- OpenVPN menyediakan manajemen interface yang dapat digunakan untuk mengkontrol secara remote atau mengatur openVPN daemon secara terpusat.
- Kelebihan openVPN adalah *cross-platform portability*, stabilitas yang sangat baik, skalabilitas yang sangat tinggi, mencapai ratusan sampai ribuan client, instalasi yang relatif mudah, dan men-*support dynamic IP address* dan *NAT*.

Selain mempunyai banyak kelebihan, OpenVPN juga memiliki kelemahan yaitu :

- Tidak kompatibel dengan IPsec, yang mana IPsec merupakan solusi dari VPN pada umumnya.
- Hanya sedikit orang yang mengetahui cara menggunakan OpenVPN, terutama dalam skenario/masalah jaringan yang sulit.
- Pada saat ini, OpenVPN hanya dapat menghubungkan komputer satu dengan komputer lain, namun ke depannya akan ada perusahaan yang mengintegrasikan *client* OpenVPN pada alat-alatnya.