BAB 2
TINJAUAN PUSTAKA

2.1 Profil Universitas Sangga Buana YPKP

Pengalaman Yayasan Pendidikan Keuangan dan Perbankan (YPKP) mengelola pendidikan lebih dari 44 tahun, semenjak 1968 mengelola Akademik Bank Nasional (ABN) Cabang Bandung, kemudian ABN berubah menjadi AKUBANK YPKP, dan berubah lagi menjadi STIE YPKP, serta mendirikan STT YPKP. Selanjutnya STIE YPKP dan STT YPKP bergabung ditambah Fakultas Ilmu Komunikasi dan Administrasi sehingga menjadi Universitas Sangga Buana YPKP.

Pendirian USB YPKP bertujuan mencerdaskan kehidupan bangsa dan menunjang nilai-nilai luhur bangsa dalam mengelola program pendidikan dari Diploma, Sarjana dan Pascasarjana dalam upaya mencapai masyarakat adil, makmur dan sejahtera yang diridhoi oleh Allah SWT.

Universitas Sangga Buana Yayasan Pendidikan Keuangan dan Perbankan, yang disingkat USB YPKP berdiri sejak dikeluarkannya Surat Keputusan DIKTI nomor 178/D/O/2006, tanggal 24 Agustus 2006, terdiri dari tiga Fakultas, yang merupakan hasil penggabungan Sekolah Tinggi Ilmu Ekonomi (STIE) YPKP (sekarang menjadi Fakultas Ekonomi USB YPKP) dengan Sekolah Tinggi Teknologi (STT) YPKP (sekarang menjadi Fakultas Teknik USB YPKP), ditambah dengan pendirian Fakultas baru, yaitu Fakultas Ilmu Komunikasi dan Administrasi (FIKA).

2.1.1 Sejarah Singkat Universitas Sangga Buana YPKP

Wujud embrional STIE YPKP adalah Akademi Bank Nasional (ABN) Cabang Bandung yang didirikan pad tanggal 23 Maret 1968 sebagai cabang dari ABN Jakarta.

Berdasarkan suatu persetujuan bersama pada tanggal 21 Februari 1970, Akademi Bank Nasional (ABN) Cabang Bandung ini diserahkan kepada Yayasan Pendidikan Keuangan dan Perbankan (YPKP), selanjutnya berubah menjadi Akademi Bank YPKP dengan status "Terdaftar" sesuai dengan surat Keputusan Menteri Pendidikan dan Kebudayaan Nomor 201/DPT/I/1970, tanggal 15 April 1970. Pada tahun 1979 Akademi Bank YPKP membuka jurusan Akuntansi. Adanya penambahan jurusan ini, maka Akademi Bank YPKP berubah nama menjadi Akademi Keuangan dan Perbankan YPKP (AKUBANK YPKP).

Sesuai dengan Surat Keputusan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 0317/0/1981, tanggal 24 oktober 1981, AKUBANK YPKP memiliki status "Diakui" untuk jurusan Perbankan dan Status "Terdaftar" untuk jurusan Akuntansi.

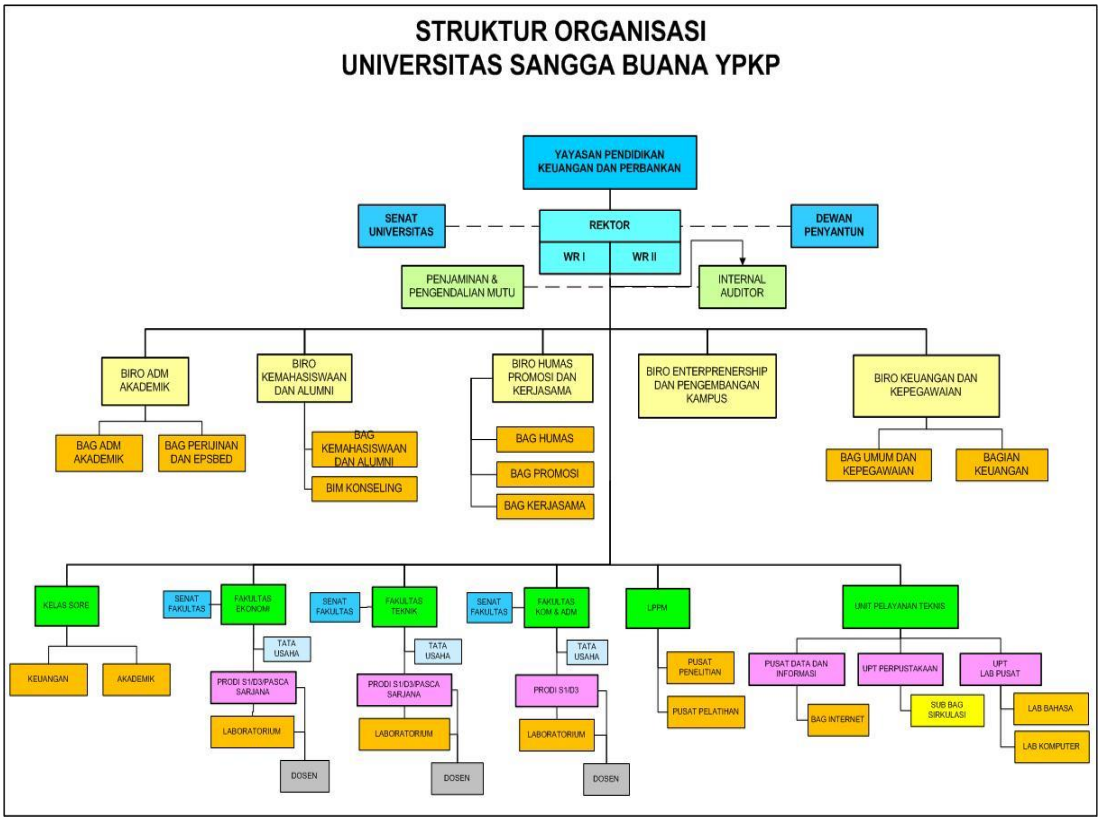
Berdasarkan Keputusan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 0336/0/1984, tanggal 9 Agustus 1984 tentang penataan jurusan dan program studi pada Perguruan Tinggi, maka sesuai pula dengan Keputusan Badan Pengurus YPKP Nomor 034/I/YPKP/84, tanggal 10 November 1984, Nomor 068A/I/YPKP/85 tanggal 3 April 1985, AKUBANK YPKP ditingkatkan Status dan Jenjang Programnya menjadi Sekolah Tinggi Ilmu Ekonomi Yayasan Pendidikan Keuangan dan Perbankan (STIE YPKP).

2.1.2 Tempat dan Kedudukan Universitas Sangga Buana YPKP

Universitas Sangga Buana YPKP bertempat di Jl. PHH. Mustopa No. 68 Telp. 022-7275489, 7202841 Fax. 022-7201756 BANDUNG 40124.

2.1.3 Struktur Organisasi Universitas Sangga Buana YPKP

Struktur organisasi merupakan susunan yang terdiri dari fungsi-fungsi dan hubungan- hubungan yang menyatakan keseluruhan kegiatan untuk mencapai suatu sasaran. Struktur keorganisasian pada Universitas Sangga Buana YPKP dapat dilihat pada gambar 2.1.



Gambar 2.1. Struktur Organisasi Universitas Sangga Buana YPKP.

Keterangan :

PIMPINAN REKTORAT

Rektor

Dr. H. Asep Effendi, SE., SE., MSi.

Wakil Rektor I (Bidang Akademik & Kemahasiswaan)

Dr. H. Vip Paramarta, Drs., MM.

Wakil rektor II (Bidang Keuangan & Adm. Umum)

Memi Sulaksmi, SE., MSi.

PIMPINAN DEKANAT

Fakultas Ekonomi :

Dekan : H. Dadang Saeful Hidayat, SE,. MM.

Wakil Dekan : Heti Herawati, SE., MSi.

Fakultas Komunikasi & Administrasi :
Dekan : Prof. Dr. H. Tachjan, Drs, M.Si.
Wakil Dekan : Dr. Atang Syamsudin, Drs.

Fakultas Teknik :
Dekan : Dr. H. Bachtiar, Ir, MT.
Wakil Dekan : Tia Sugiri, Drs, ST, M.Pd.

Program Pascasarjana :
Magister Manajemen : Dr. H. Deden Sutisna MN, SE, M.Si.
Magister Teknik : Dr. R. Didin Kusdian, Ir., M.T.

2.1.4 *Job Description*

Badan Penyelenggara (BP) Yayasan Pendidikan Keuangan dan Perbankan (YPKP)**.**

Yayasan Pendidikan Keuangan dan Perbankan (YPKP) adalah Badan Penyelenggara yang mendirikan dan membina serta mngembangkan perguruan tinggi swasta, dalam hal ini Universitas Sangga Buana (USB) YPKP.

Organisasi Yayasan Pendidikan Keuangan dan Perbankan (YPKP)

1. Pembina YPKP

Pembina YPKP merupakan organisasi Yayasan yang mempunyai kewenangan yang tidak diserahkan kepada Pengurus atau Pengawas oleh Undang-undang tentang Yayasan atau Anggaran Dasar.

Adapun kewenangan Pembina YPKP meliputi :

a. Keputusan mengenai perubahan Anggaran Dasar YPKP.
b. Pengangkatan dan pemberhentian anggota Pengurus dan Pengawas YPKP.
c. Penetapan kebijakan umum Yayasan berdasarkan Anggaran Dasar Yayasan.
d. Pengesahan program kerja dan rancangan anggaran tahunan Yayasan.
e. Penetapan keputusan mengenai penggabungan atau pembubaran Yayasan.

2. Pengurus YPKP

Pengurus YPKP adalah organisasi Yayasan yang melaksanakan kepengurusan Yayasan dan tidak merangkap sebagai Pembina atau Pengawas.

Pengurus YPKP diangkat oleh Pembina YPKP berdasarkan keputusan rapat Pembina untuk jangka waktu selama 5 (lima) tahun dan dapat diangkat kembali untuk 1 (satu) kali masa jabatan.

Susunan Pengurus YPKP terdiri atas :

a. Seorang Ketua.

b. Seorang Sekretaris.

c. Seorang Bendahara.

3. Pengawas YPKP

Pengawas YPKP adalah organisasi Yayasan yang bertugas melakukan pengawasan serta memberi nasihat kepada Pengurus dalam menjalankan kegiatan Yayasan. Pengawas diangkat oleh Pembina berdasarkan keputusan rapat Pembina untuk jangka waktu 5 (lima) tahun dan dapat diangkat kembali untuk 1 (satu) masa jabatan. Pengawas tidak boleh merangkap sebagai Pembina atau Pengurus Yayasan. Segala wewenang, tugas dan tanggung jawab pengawas YPKP diatur dalam Anggaran Dasar YPKP.

2.1.5 Visi dan Misi Universitas Sangga Buana YPKP

2.1.5.1 Visi

VISI menjadi Pendidikan Tinggi Ilmu Ekonomi unggulan (*centre of excellence*) yang bertaraf Internasional dalam bidang Manajemen, Akuntansi, serta Keuangan dan Perbankan sehingga menjadi salah satu Perguruan Tinggi Ilmu Ekonomi terkemuka di Indonesia.

2.1.5.2 Misi

1. Menyelenggarakan Pendidikan Ilmu Ekonomi bidang Manajemen, Akuntansi, serta Keuangan secara profesional sesuai dengan

perkembangan ilmu pengetahuan dan teknologi yang menghasilkan tenaga terdidik yang berahlak mulia dan memiliki daya saing global.

2. Membangun *scientific atmospheree* yang berbasis pada ilmu Manajemen, Akuntansi, serta Keuangan dan Perbankan sesuai dengan perkembangan ilmu dan teknologi.
3. Melaksanakan pelayanan akademik secara profesional dan paripurna yang berbasis teknologi yang canggih.
4. Melaksanakan penelitian dan pengembangan ilmu ekonomi dalam bidang manajemen, Akuntansi, serta Keuangan dan Perbankan.
5. Membantu mengembangkan kehidupan masyarakat dengan menerapkan ilmu pengetahuan dan teknologi yang relevan.

2.1.6 Tujuan

Mencerdaskan kehidupan bangsa dan menunjang nilai-nilai luhur bangsa dalam mengelola program pendidikan dari Diploma, Sarjana dan Pascasarjana dalam upaya mencapai masyarakat adil, makmur dan sejahtera yang diridhoi oleh Allah SWT.

2.1.7 Logo Universitas Sangga Buana YPKP



Gambar 2.2. Logo Universitas Sangga Buana YPKP.

2.2 Landasan Teori

Landasan teori menjelaskan dasar-dasar teori yang digunakan dalam penelitian yang dilakukan pada tugas akhir. Teori-teori yang digunakan meliputi antara lain Jaringan Komputer, Topologi Jaringan, *Transmission Control Protocol/ Internet Protocol (tcp/ip),* Sejarah IPCop, *Firewall*, *Virtual Private Network* (VPN), *Spoofing*, *SYN Flood* dan Metode *Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle*.

2.2.1 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas beberapa komputer yang didesain sedemikian rupa sebagaimana tujuan utamanya yakni untuk dapat berbagi sumber daya (CPU, *printer*), berkomunikasi (pesan *instan*). Tujuan dibangunnya suatu jaringan komputer adalah untuk membawa data informasi dari sisi pengirim menuju penerima secara cepat dan tepat tanpa adanya kesalahan melalui media transmisi atau media komunikasi tertentu.

2.2.1.1 Jenis-Jenis Jaringan Komputer

Jaringan komputer yang digunakan saat ini dapat dikelompokkan berdasarkan area yang dapat dijangkau. Area ini mulanya ditentukan berdasarkan jarak jangkau dalam satuan meter. Namun dalam perkembangan selanjutnya berdasarkan peralatan dan fasilitas. Penggunaan peralatan–peralatan yang dimaksud adalah peralatan–peralatan *internet* jaringan seperti *repeater*, *router* atau *gateway* dari peralatan tersebut dapat dilihat jangkauan area jaringan dan luasan segmen jaringan yang dibangun.

Berdasarkan kriteria–kriteria tersebut secara umum jaringan komputer dapat digolongkan sebagai Berikut ini merupakan :

1. *Local Area Network (LAN)*
2. *Metropolitan Area Network (MAN)*
3. *Wide Area Network (WAN)*
4. *Wireless Network*

***a. Local Area Network* (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. LAN mempunyai ukuran yang terbatas, yang berarti bahwa waktu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui keterbatasnnya, menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu.

***b. Metropolitan Area Network* (MAN)**

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar.

***c. Wide Area Network* (WAN)**

Wide Area Network (WAN) merupakan jenis jaringan yang lebih luas dan lebih canggih daripada LAN dan MAN. Teknologi jaringan WAN biasa digunakan untuk menghubungkan suatu jaringan dengan negara lain atau dari satu benua ke benua yang lainnya. Jaringan WAN bisa terdiri dari berbagai LAN dan WAN karena luasnya wilayah cakupan dari WAN. Jaringan WAN, biasanya menggunakan kabel *fiber optic* serta menanamkannya di dalam tanah maupun melewati jalur bawah laut.

d. Wireless Network

Wireless Network merupakan peralatan *end-user* untuk megakses jaringan dengan menggunakan transmisi radio pendek atau sedang.

Wireless WAN : GSM (sampai 20 Kbps)

Wireless LAN/MAN : WaveLAN (2-11 Mbps, sampai 150 m)

Wireless PAN (*Personal Area Network*) : *Bluetooth (*sampai 2 Mbps, jarak < 10 m)

2.2.1.2 Tipe-Tipe Jaringan Komputer

Dalam jaringan komputer terdapat dua tipe jaringan, yaitu :

1. Model *client-server.*
2. Model *peer to peer* atau *point to point.*

a. Jaringan *Client-Server*

Jaringan *Client-Server* adalah Jaringan komputer dengan komputer yang didedikasikan khusus sebagai *server*. Sebuah *service*/layanan bisa diberikan oleh sebuah komputer atau lebih. Konsep Jaringan *client-server* ini membedakan dengan jelas kedudukan suatu komputer, mana yang dapat memberikan layanan jaringan (*server*) dan mana yang hanya meminta layanan (*client*). Jika suatu komputer di*install* sebagai *server* yang memberikan segala sumber daya (*resource*), contohnya : *printer*, *modem* kepada komputer lain (*client)* yang terhubung ke jaringan. Untuk dapat saling berkomunikasi antara *server* dan *client*, maka digunakan suatu aplikasi jaringan yang dinamakan *client-server program*, dimana *server* menggunakan aplikasi jaringan yang disebut *server program*, sementara *client* menggunakan *client program* untuk dapat berkomunikasi dengan *server program* pada *server*.

Beberapa sifat dari *client-server* diantaranya sebagai Berikut ini merupakan :

a. *Server* dan *Client* berada pada posisi serta proses yang berbeda.
b. *Server* dan *Client* dapat dijalankan pada mesin yang sama atau berbeda.
c. Setiap proses dapat menyembunyikan informasi tersendiri.
d. Komunikasi yang dilakukan bisa bersifat protokol *peer to peer*.

Konektivitas *client ke Server :*

a. *Server* harus terlebih dahulu dijalankan (*running*).
b. *Server* harus menentukan *port* untuk koneksi yang masuk.
c. *Client* harus mengetahui nama *Host* dari *server* beserta *port* yang digunakan untuk koneksi.
d. *Client* mengirim pesan ke *server* untuk melakukan suatu pekerjaan (*task*). *Server* dan *Client* bersifat *Asimetrik.*

Tabel 2.1. Keunggulan dan Kelemahan *Client-Server.*

KEUNGGULAN	KELEMAHAN
Kecepatan akses lebih tinggi karena penyediaan fasilitas jaringan dan pengelolaannya dilakukan secara khusus oleh satu komputer (*server*) yang tidak dibebani dengan tugas lain sebagai *workstation*.	Biaya operasional relatif lebih mahal.
Sistem keamanan dan administrasi jaringan lebih baik, karena terdapat seorang pemakai yang bertugas sebagai administrator jaringan, yang mengelola administrasi dan sistem keamanan jaringan.	Diperlukan adanya satu komputer khusus yang berkemampuan lebih untuk ditugaskan sebagai *server*.
Sistem *backup* data lebih baik, karena pada jaringan *client-server backup* dilakukan terpusat di *server*, yang akan membackup seluruh data yang digunakan di dalam jaringan.	Kelangsungan jaringan sangat tergantung pada *server*. Bila *server* mengalami gangguan maka secara keseluruhan jaringan akan terganggu.

b. Jaringan *Peer to peer*

Pada model jaringan terdapat hanya dua komputer yang saling terhubung. Masing-masing komputer mempunyai kedudukan yang setara atau setingkat sehingga komputer manapun dapat memulai (*initiate*) dan mengendalikan hubungan dalam jaringan. Model Jaringan ini merupakan jenis yang paling sederhana. Berikut ini merupakan kelebihan dan kekurangan dari jaringan *peer to peer.*

Tabel 2.2. Keunggulan dan Kelemahan *peer to peer.*

KEUNGGULAN	KELEMAHAN
Antar komputer dalam jaringan dapat saling berbagi-pakai fasilitas yang dimilikinya seperti *harddisk, drive, fax/modem, printer*.	*Troubleshooting* jaringan relatif lebih sulit, karena pada jaringan tipe *peer to peer* setiap komputer dimungkinkan untuk terlibat dalam komunikasi yang ada. Di jaringan *client-server*, komunikasi adalah antara *server* dengan *workstation*.
Biaya operasional relatif lebih murah dibandingkan dengan tipe jaringan *client-server*, salah satunya karena tidak memerlukan adanya *server* yang memiliki kemampuan khusus untuk mengorganisasikan dan menyediakan fasilitas jaringan.	Unjuk kerja lebih rendah dibandingkan dengan jaringan *client-server*, karena setiap komputer disamping harus mengelola pemakaian fasilitas jaringan juga harus mengelola pekerjaan atau aplikasi sendiri.
Kelangsungan kerja jaringan tidak tergantung pada satu *server*. Sehingga bila salah satu komputer/peer mati atau rusak, jaringan secara keseluruhan tidak akan mengalami gangguan.	Sistem keamanan jaringan ditentukan oleh masing-masing user dengan mengatur keamanan masing-masing fasilitas yang dimiliki.

2.2.2 Topologi Jaringan Komputer

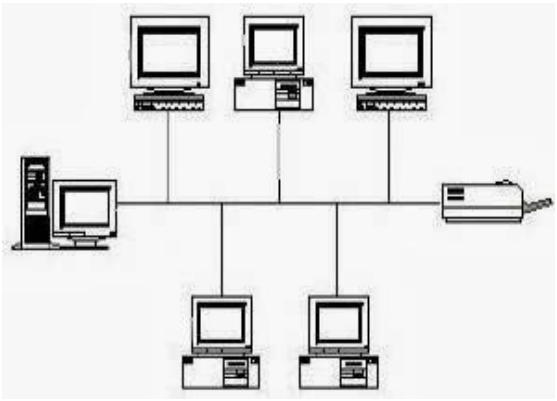
Topologi jaringan merupakan suatu struktur atau bagaimana menghubungkan antara simpul dan pusat dalam suatu jaringan. Tiap struktur mempunyai keuntungan dan kerugiannya masing-masing.

Bentuk-bentuk arsitektur jaringan komputer secara fisik adalah sebagai Berikut ini merupakan :

1. Topologi *Bus.*
2. Topologi *Star.*
3. Topolgi *Tree.*
4. Topologi *Ring.*

2.2.2.1 Topologi *Bus*

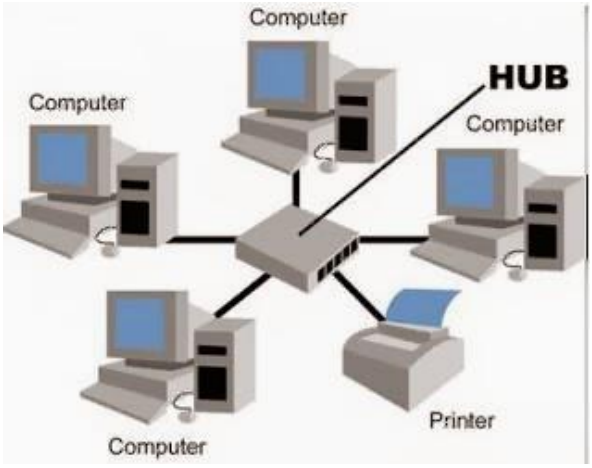
Topologi sebuah bus merupakan garis lurus yang terdiri dari satu jalur kabel utama (*backbone*) dimana pada masing-masing ujungnya diberikan sebuah *terminator*. Semua *nodes* pada jaringan (*file server, workstation*, dan perangkat lainnya) terkoneksi ke sebuah kabel utama. Jaringan-jaringan *Ethernet* dan *Localtalk* menggunakan topologi *linear* ini.



Gambar 2.3. Topologi *Bus.*

2.2.2.2 Topologi *Star*

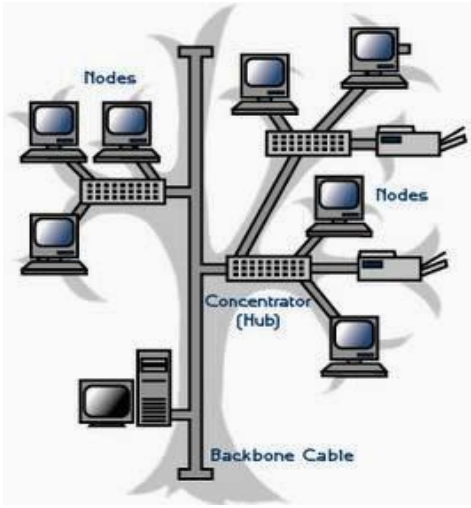
Topologi model ini didesain dimana setap *node* (*file server, workstation*, dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah *concentrator* baik berupa *HUB* ataupun *SWITCH*. Data yang terkirim ke jaringan akan melewati *concentrator* sebelum melanjutkan ke tempat tujuannya. *Concentrator* akan mengatur dan mengontrol keseluruhan fungsi jaringan. Dia juga bertindak sebagai *repeater* dalam skala kecil dari aliran data. Konfigurasi pada jaringan model ini menggunakan kabel *Twisted Pair*.



Gambar 2.4. Topologi *Star.*

2.2.2.3 Topologi *Tree*

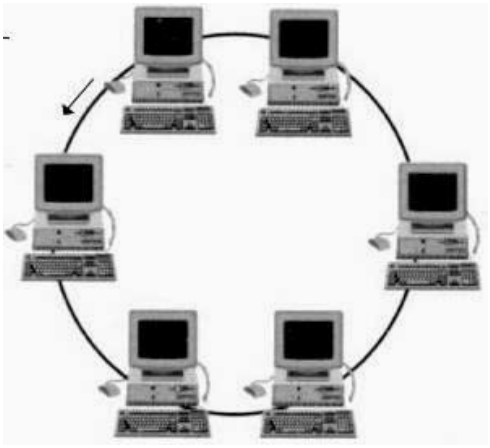
Sebuah topologi model ini merupakan perpaduan antara topologi *Linear BUS* / Garis Lurus dan Bintang, yang terdiri dari kelompok-kelompok dari *workstation* konfigurasi Bintang yang terkoneksi ke kabel utama yang menggunakan topologi *Linear BUS* / Garis Lurus. Topologi ini memungkinkan untuk pengembangan jaringan yang telah ada, dan memungkinkan sebuah perusahaan mengkonfigurasi jaringan sesuai dengan kebutuhannya. Berikut ini merupakan gambar topologi *tree.*



Gambar 2.5. Topologi *Tree.*

2.2.2.4 Topologi *Ring*

Dalam topologi *Ring* semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat- alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan.



Gambar 2.6. Topologi *Ring.*

2.2.3 *Transmission Control Protocol / Internet Protocol (TCP/IP)*

2.2.3.1 Sejarah TCP/IP

Internet Protocol dikembangkan pertama kali oleh *Defense Advanced Research Projects Agency* (DARPA) pada tahun 1970 sebagai awal dari usaha untuk mengembangkan protokol yang dapat melakukan interkoneksi berbagai jaringan komputer yang terpisah, yang masing-masing jaringan tersebut menggunakan teknologi yang berbeda. Protokol utama yang dihasilkan proyek ini adalah *Internet Protocol* (IP). Riset yang sama dikembangkan pula yaitu beberapa protokol level tinggi yang didesain dapat bekerja dengan IP. Yang paling penting dari proyek tersebut adalah *Transmission Control Protocol* (TCP), dan semua grup protokol diganti dengan TCP/IP *suite*. Pertama kali TCP/IP diterapkan di ARPANET, dan mulai berkembang setelah Universitas California di Berkeley mulai menggunakan TCP/IP dengan sistem operasi UNIX. Selain *Defense*

Advanced Research Projects Agency (DARPA) ini yang mengembangkan *Internet Protocol*, yang juga mengembangkan TCP/IP adalah *Department of Defense* (DOD).

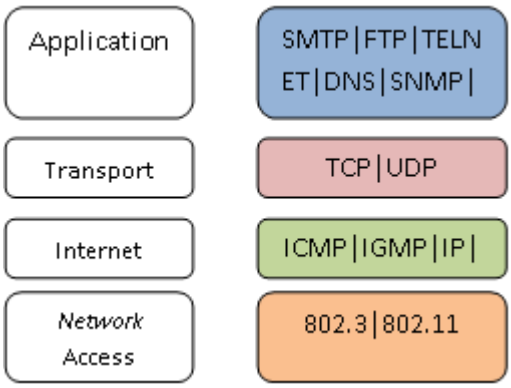
2.2.3.2 Standar TCP/IP

TCP/IP adalah sekumpulan protokol yang mengatur komunikasi data komputer di internet, komputer-komputer yang terhubung di internet berkomunikasi dengan protokol ini, karena menggunakan protokol yang sama maka perbedaan jenis komputer dan system operasi tidak terjadi masalah. Perkembangan protokol TCP/IP yang diterima luas dan praktis menjadi *standar de facto* jaringan komputer berkaitan denga ciri-ciri yang terdapat pada protokol itu sendiri yaitu :

1. Protokol TCP/IP dikembangkan menggunakan standar protokol terbuka (*open system*).
2. Standar protokol TCP/IP dalam bentuk *Request For Comment* (RFC) dapat digunakan oleh siapapun.
3. TCP/IP dikembangkan dengan tidak tergantung pada perangkat lunak atau perangkat keras tertentu.
4. Pengembangan TCP/IP dilakukan dengan konsensus dan tidak tergantung pada vendor tertentu.
5. TCP/IP *independent* terhadap perangkat keras, jaringan dan dapat dijalankan pada jaringan *Ethernet*, *token ring*, jalur telpon *Dial-up* dan praktis media apapun.
6. Pengalamatan TCP/IP bersifat unik dalam skala global. Dengan cara ini, komputer dapat saling terhubung walaupun jaringannya seluas internet sekarang ini.
7. TCP/IP memiliki fasilitas *routing* sehingga dapat diterapkan pada internet, dan memiliki jenis layanan lainnya.

2.2.3.3 Model TCP/IP

TCP/IP terbentuk dari empat layer (lapisan) kumpulan protokol yang bertingkat yaitu *Application layer, Transport layer, Internet layer, dan Network Access layer*.



Gambar 2.7. Model TCP/IP.

Keterangan *layer* pada TCP/IP adalah :

1. *Layer Aplikasi* adalah sebuah aplikasi yang mengirimkan data ke transport layer. Misalnya :
   a. *Domain Name Service Protocol (DNS)* digunakan untuk meresolve nama di internet menjadi alamat IP.
   b. *Hypertext Transfer Protocol (HTTP)* digunakan untuk transfer file-file halaman web di *world wide web (www).*
   c. *Telnet* merupakan suatu terminal emulator yang disediakan untuk *remote access* ke *server* atau ke perangkat jaringan lainnya.
   d. *File Transfer Portovol (FTP)* digunakan untuk mentransfer file antar system.
   e. *Simple Network Management Protocol (SNMP)* merupakan protokol standar industri yang digunakan untuk memonitor dan mengelola berbagai perangkat di jaringan internet meniputi *hub, rotuter, switch, workstation,* dan sistem manajemen jaringan secara jarak jauh (*remote*).
   f. *Simple Mail Transfer Protocol (SMTP)* digunakan untuk transfer file surat elektronik dan *attachment.*
2. *Layer Transport* bertanggung jawab untuk komunikasi antara aplikasi. Layer ini mengatur aluran informasi dan mungkin menyediakan pemeriksaan error. Data dibagi kedalam beberapa paket yang dikirim ke internet layer dengan sebuah *header. Header* mengandung alamat tujuan, alamat sumber dan *checksum*. *Checksum* diperiksa oleh mesin penerima untuk melihat apakah paket tersebut ada yang hilang pada rute.

Tabel 2.3. Perbedaan TCP / UDP.

TCP	UDP
Reliable	*Unreliable*
Connection-oriented	*connectionless*
Segment retransmission and flow control through windowing	*No windowing or retransmission*
Segment sequencing	*No sequencing*
Acknowledge segments	*No acknowledge*

1. *Layer Internet* bertanggung jawab untuk komunikasi antara mesin. Layer ini meg-*encapsul* paket dari transport layer ke dalam IP datagrams dan menggunakan algoritma *routing* untuk menentukan kemana datagaram harus dikirim. Masuknya datagram diproses dan diperiksa kesahannya sebelum melewatinya pada *Transport layer*.
2. *Layer Networks Access* adalah level yang paling bawah dari susunan TCP/IP. Layer ini adalah device driver yang memungkinkan datagaram IP dikirim ke atau dari fisikal *network*. Jaringan dapaat berupa sebuah kabel, *Ethernet, frame relay, Token ring, ISDN*, ATM jaringan, radio, satelit atau alat lain yang dapat mentransfer data dari sistem ke sistem. Layer *network interface* adalah abstraksi yang memudahkan komunikasi antara *multitude arsitektur network.*

Dalam TCP/IP terjadi penyampaian data dari protokol yang berada di suatu layer ke protokol yang berada di layer lain. Jika suatu protokol menerima data dari protokol lain di layer diatasnya, protokol ini akan menambahkan informasi tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan protokol tersebut.

2.2.4 Sejarah Singkat IPCOP

IPCop Linux adalah distribusi *software* yang bertujuan untuk menyediakan cara yang mudah untuk mengatur *firewall* berbasis perangkat keras PC. IPCop adalah sebuah *firewall* yang dibangun di atas kerangka Linux *Netfilter*. Distro ini awalnya dikembangkan oleh tim yang mengembangkan *Smoothwall Linux firewall*, perkembangan selanjutnya, proyek IPCop dikembangkan dengan bebas, dan saat ini sudah terpisah sepenuhnya. IPCop sangat *simple*, dan memiliki fitur *user-managed* untuk mekanisme *update security*-nya. Bahkan cenderung mudah dipahami untuk yang para pemula, dan handal untuk yang sudah berpengalaman.

IPCop dikembangkan secara *Opensource*, dengan komunitas pengembang *independent* yang tersebar diseuluruh dunia. *CD-ROM image* untuk instalasi dapat dengan mudah di download dan memiliki miror yang cukup banyak. Pengembangan IPCop terus berlanjut hingga saat ini sudah mencapai seri rilis 1.4.x. Sekarang sudah dirilis versi 1.4.21 dibulan Juli 2008. saat ini sedang dikembangkan IPCop Version 2.0.

2.2.4.1 Fitur-Fitur IPCop

Fitur-fitur yang dimiliki IPCop yaitu sebagai berikut:

1. Aman, stabil dan merupakan Linux *based firewall* yang sangat mudah dikonfigurasi.
2. Mudah untuk melakukan Administrasi lewat *web* akses.
3. IPCop dapat menggunakan DHCP IP *address* dari ISP yang digunakan.
4. Dapat berfungsi sebagai DHCP *server* untuk memudahkan konfigurasi *internal network.*
5. Memiliki kemampuan sebagai *caching* DNS *proxy*, untuk membantu menambah kecepatan *query Domain Name*.
6. Memiliki *web caching proxy*, untuk menambah kecepatan akses *web*.
7. Sebagai *intrusion detection system* untuk mendeteksi serangan ke *internal network* yang digunakan.

8. Kemampuan untuk memisahkan *network*, konfigurasi *GREEN* untuk *internal network* yang aman, *network* terlindungi dari internet, konfigurasi *BLUE* untuk *network* dengan *wireless* LAN dan a DMZ or *ORANGE* untuk *network* yang diperbolehkan diakses oleh publik seperti *webserver/mailserve*.
9. Fasilitas VPN yang digunakan untuk koneksi ke *internal network* dari eksternal *network* melalui internet secara aman karena telah ditingkatkan untuk *support x509 certificates.*
10. Memiliki *Traffic shaping* untuk mengatur prioritas *service* seperti *web browsing, FTP, telnet* dan lain-lain sesuai keinginan.
11. Dibangun dengan *ProPolice* untuk mencegah serangan pada semua aplikasi.
12. Memiliki pilihan konfigurasi kernel yang mengizinkan kita memilih sesuai dengan keadaan yg kita inginkan.

2.2.4.2 Konfigurasi IPCop

Network Interface IPCop terdefinisi atas empat macam yaitu RED, GREEN, BLUE dan ORANGE yaitu sebagai berikut:

1. RED *Network Interface*

   Network ini adalah *interface* internet atau *untrusted network*. Pada dasarnya yang dilindungi oleh IPCop adalah *network* GREEN, BLUE dn ORANGE dari *traffic* yang berasal dari *network* RED.
2. GREEN *Network Interface*

   Interface ini hanya terhubung ke komputer yang dilindungi oleh IPCop. Atau lebih dikenal dengan istilah *local network*. *Traffic* ke *interface* ini diarahkan lewat LAN *card* yang terpasang di IPCop *firewall*.
3. BLUE *Network Interface*

   Interface ini adalah *interface* pilihan (digunakan jika dibutuhkan) yang dapat digunakan untuk koneksi perangkat *wireless* di *network* yang berbeda dari *local network*. Komputer dibawah *interface* ini tidak dapat

terhubung dengan komputer yang berada di *interface* GREEN kecuali dikontrol menggunakan ‘pinholes’ atau *via* koneksi VPN. *Traffic* ke *interface* ini juga diarahkan lewat LAN *card* yang terpasang di IPCop *firewall*.

4. ORANGE *Network Interface*

   Interface ini juga merupakan *interface* pilihan yang digunakan untuk menempatkan *server* yang boleh diakses oleh *network* yang berbeda. Komputer dibawah *interface* ini tidak dapat terhubung dengan komputer yang berada di *interface* GREEN atau BLUE kecuali dikontrol menggunakan ‘DMZ pinholes’. *Traffic* ke *interface* ini juga diarahkan lewat LAN *card* yang terpasang di IPCop *firewall*.

2.2.4.3 Konfigurasi RED, ORANGE, BLUE, GREEN

Kebutuhan *Network Interfaces Card* yaitu IPCop *firewall* kita setidaknya membutuhkan 1 *network ethernet card* (NIC) dan satu kabel jaringan. Bisa jadi kita membutuhkan sampai 4 NIC, bergantung dari konfigurasi *network* yang dipilih dan koneksi internet yang digunakan.Seluruh NIC harus berbeda secara fisik.

Abaikan untuk *network* RED, kita dapat menghubungkan NIC dan kabel *network* yang berbeda ke IPCop untuk *network* GREEN, BLUE dan/atau ORANGE. *Network* GREEN dan RED merupakan keharusan, sedangkan ORANGE dan BLUE merupakan pilihan. Kebutuhan *interface* untuk *network* RED bervariasi bergantung koneksi internet yang kita gunakan, apakah menggunakan NIC atau Modem.

Tipe konfigurasi *network* IPCop dasar yang digunakan adalah RED/GREEN, dimana IPCop melindungi *internal network* (GREEN) dari internet. Jika kita memiliki *wireless access point*, kita dapat menghubungkannya ke *interface* BLUE dan mengkonfigurasi IPCop untuk membatasi akses di *wireless* LAN tersebut. Jika kita memiliki beberapa *server* yang diperbolehkan diakses *via* internet, dapat kita letakkan di *untrusted* DMZ pada *interface*

ORANGE. *Interface* RED dapat dihubungkan dengan modem atau NIC, terdapat delapan Tipe Konfigurasi *Network*, yaitu:

1. GREEN (RED adalah modem/ISDN)
2. GREEN + RED (RED adalah *Ethernet*)
3. GREEN + ORANGE + RED (RED adalah *Ethernet*)
4. GREEN + ORANGE (RED adalah modem/ISDN)
5. GREEN + BLUE + RED (RED adalah *Ethernet*)
6. GREEN + BLUE (RED adalah modem/ISDN)
7. GREEN + BLUE + ORANGE + RED (RED adalah *Ethernet*)
8. GREEN + BLUE + ORANGE (RED adalah modem/ISDN)

2.2.4.4 Kebutuhan Network Interfaces Card (NIC)

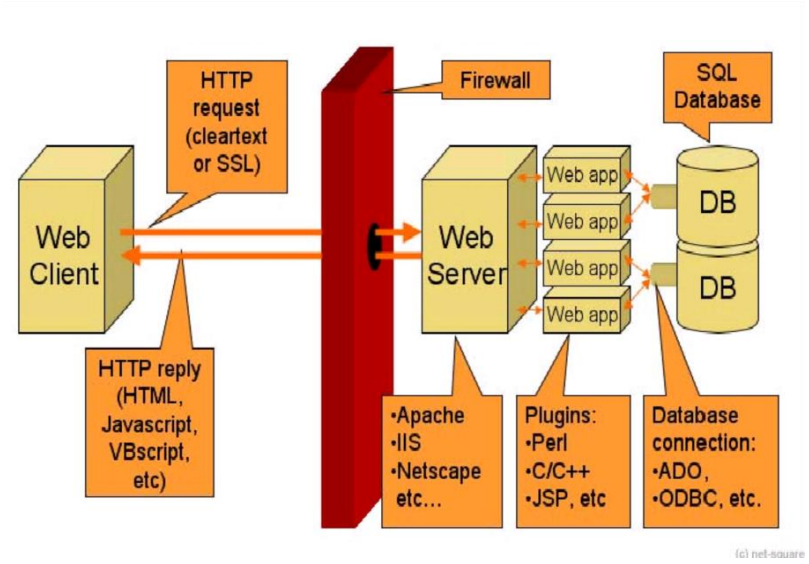
Model *security* IPCop didalam *network* GREEN adalah *fully trusted* dan *request* dari *network in*, mungkin dari *user* atau dari komputer yang terinfeksi *virus, trojan horse* atau *malware* adalah sah dan diperbolehkan lewat oleh IPCop.

Dalam fitur baru pada IPCop 1.4.x, terdapat *Intrusion Detection System* (IDS) untuk seluruh *interface*. Hal ini merupakan ide bagus untuk mendeteksi kondisi *internal network* jika terdapat indikasi infeksi *virus* atau *malware*.

2.2.5 Pengertian Firewall

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah *firewall* diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. *Firewall* umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah *firewall* menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan

tersebut dari serangan para *hacker*, pelaku *spionase*, ataupun pencuri data lainnya, menjadi esensial. Contoh ilustrasi *firewall* diperlihatkan pada gambar 2.8.



Gambar 2.8. Ilustrasi Firewall.

2.2.5.1 Fungsi firewall

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan.

   Firewall harus dapat mengatur, mem-*filter* dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan *private* yang dilindungi *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan *private*.

   Beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain :

   a. Alamat IP dari komputer sumber.

   b. Port TCP/UDP sumber dari sumber.

   c. Alamat IP dari komputer tujuan.

   d. Port TCP/UDP tujuan data pada komputer tujuan.

   e. Informasi dari *header* yang disimpan dalam paket data.

2. Melakukan autentifikasi terhadap akses.

3. Applikasi *proxy*

   Firewall mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan

   Mencatat setiap transaksi kejadian yang terjadi di *firewall*. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

2.2.5.2 Cara Kerja Firewall

Cara kerja *firewall* pada umumnya:

1. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
2. Menolak dan menyaring paket data yang berasal dari jaringan *internal* ke internet. Contohnya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
3. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan. Misalnya *firewall* yang terintegrasi pada suatu antivirus akan menyaring dan mencegah *file* yang sudah terjangkit *virus* yang mencoba memasuki jaringan *internal.*
4. Melaporkan semua aktivitas jaringan dan kegiatan *firewall.*

2.2.5.3 Tipe-tipe Firewall

Tipe-tipe *Firewall,* antara lain:

1. *Packet-Filtering Firewall*

   Packet-Filtering Firewall adalah tipe *firewall* yang memeriksa dan membandingkan alamat sumber dari paket lewat dengan aturan atau kebijakan yang telah terdaftar pada *filtering firewall*. Pada *firewall* tipe ini

akan diatur apakah paket data tersebut akan diperbolehkan lewat atau menolaknya.

Aturan atau kebijakan pemeriksaan didasarkan informasi yang dapat ditangkap dari *packet header*, yaitu antara lain :

a. IP *address* sumber dan tujuan
b. Nomor port TCP/UDP sumber dan tujuan
c. Tipe ICMP *message*

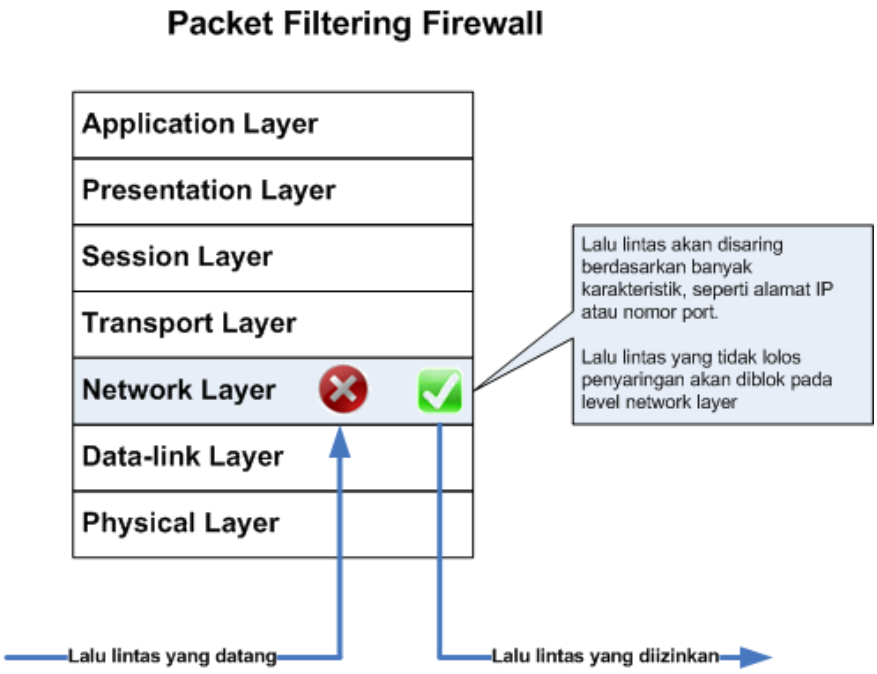
Contoh aturan atau kebijakan *packet filtering firewall* diperlihatkan pada gambar 2.9.

:

from	to	src port	dst port	proto	rule
*	www	*	80	tcp	allow
*	mail-gw	*	25	tcp	allow
squids	proxy	*	8080, 3128	*	allow
mynet	*	*	*	*	allow
*	*	*	*	*	deny

Gambar 2.9. Contoh *Rule Packet Filtering Firewall.*

Contoh ilustrasi cara kerja *packet filtering firewall* diperlihatkan pada gambar 2.10.



Gambar 2.10. Contoh Ilustrasi *Packet Filtering Firewall.*

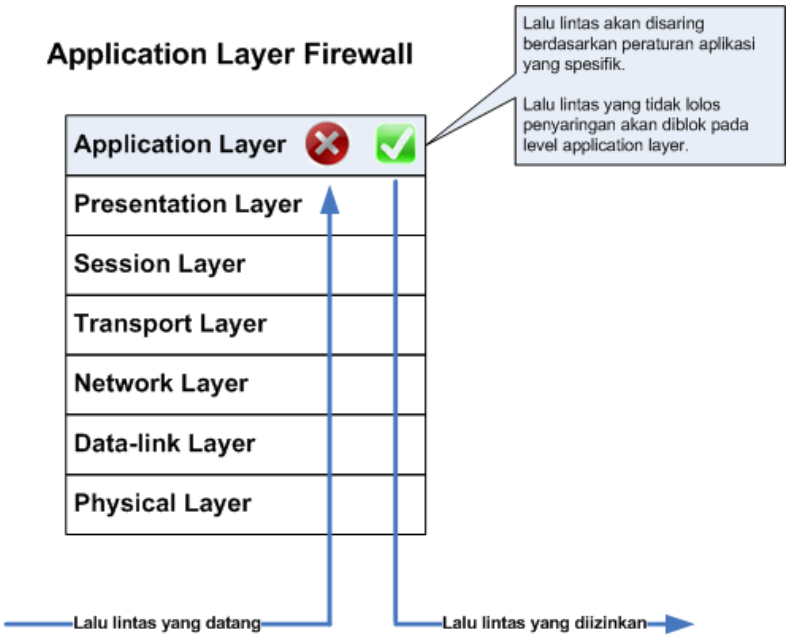
Contoh satu aturan pada *firewall* jenis adalah melakukan penonaktifan port 23 yaitu protokol yang digunakan untuk *telnet*. Ini bertujuan untuk mencegah pengguna internet untuk mengakses layanan yang terdapat pada jaringan yang di *firewall*-kan. *Firewall* ini juga dapat melakukan pengecualian terhadap aplikasi-aplikasi yang dapat berdapat berjalan di jaringan. Inilah salah satu kerumitan pada *packet filtering* tipe *firewall*, dikarena sulitnya menbuat aturan atau kebijakan yang akan diberlakuan untuk *firewall*.

Kelebihan *packet filtering firewall* antara lain relatif mudah dalam pengimplementasikannya, transparan untuk pengguna, dan relatif lebih cepat. Adapun kekurangan tipe *firewall* ini antara lain sulit dalam membuat aturan dan kebijakan pada *packet filtering firewall* ini secara tepat guna dan aturan tersebut akan semakin banyak seiiring dengan banyak alamat IP sumber dan tujuan, port sumber dan tujuan yang dimasukan dalam kebijakan *packet filtering firewall* ini.

2. *Application-Level Gateway* (*Proxy*)

Application-level gateway sering juga disebut *application level firewall* atau *proxy firewall*. *Firewall* ini tidak memperbolehkan paket data yang datang untuk melewati *firewall* sacara langsung. Application level gateway menyediakan kontrol tingkat tinggi pada *traffic* antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan difilter sesuai dengan kebijakan keamanan jaringan. *Firewall* tipe ini akan mengatur semua yang berkaitan dengan *layer* aplikasi, seperti *ftp, telner*, dll.

Kebanyakan, *proxy firewall* ini akan melakukan autentifikasi terhadap pengguna sebelum pengguna dapat melewati jaringan. *Firewall* ini juga melakukan mekanisme pencatatan (*logging*) sebagai bagian dari aturan dan kebijakan keamanan yang diterapkannya. Contohnya apabila ada pengguna salah satu aplikasi seperti *telnet* untuk mengakses secara *remote*, maka *gateway* akan meminta pengguna untuk memasukan alamat *remote host*. Ketika pengguna mengirimkan *username* dan *password* serta informasi lain maka *gateway* akan melakukan pemeriksaan dan melakukan hubungan terhadap aplikasi tersebut yang sesuai dengan *remote host*. Apabila tidak sesuai, *firewall* tidak akan meneruskan dan menolak data tersebut. Contoh ilustrasi cara kerja *application layer firewall* diperlihatkan pada gambar 2.11.



Gambar 2.11. Contoh Ilustrasi *Application Layer Firewall.*

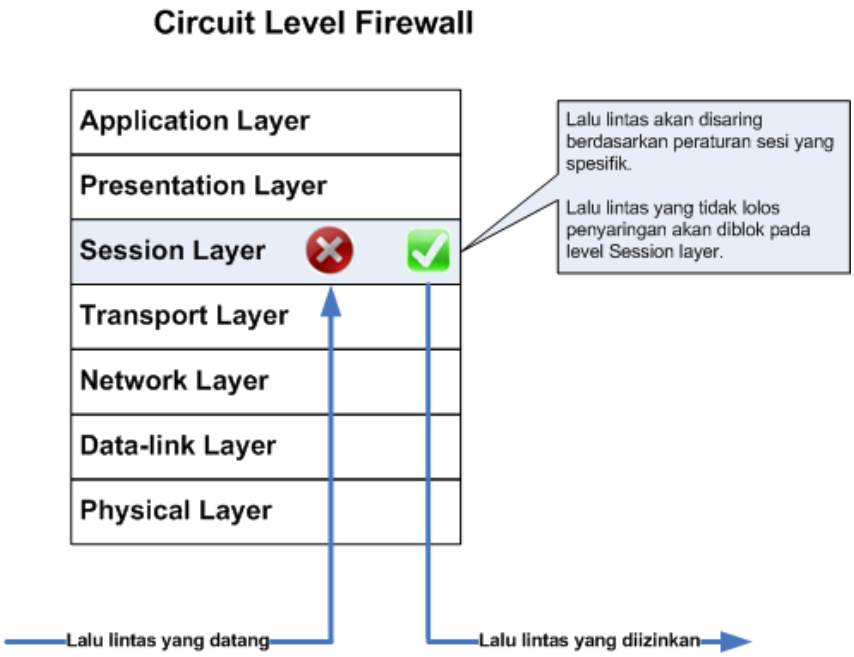
Kelebihan *application layer firewall* antara lain relatif aman dibandingkan dengan *packet filtering firewall*, adanya pencatatan *log* setiap transaksi yang terjadi pada level aplikasi.

Kekurangan *application layer firewall* antara lain pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pengguna dan *gateway*, dimana *gateway* akan memeriksa dan meneruskan semua arus dari dua arah.

3. *Circuit Level Gateway*

Circuit lavel gateway dapat dikatakan sebagai tipe khusus dari *proxy* karena *proxy* dapat dikonfigurasi untuk melewatkan semua informasi pengguna yang sudah di authentifikasi sebagai *circuit level gateway*. *Circuit level gateway* meng-*handle* koneksi TCP dan tidak menyediakan paket tambahan seperti *processing* atau *filtering*. *Firewall* jenis akan menyembunyikan jaringan dari pengguna ketika koneksi akan terjadi dari pengguna. Pengguna akan berhadapan langsung dengan *firewall* pada saat proses pembuatan koneksi dan *firewall* akan membentuk koneksi dengan

sumber daya di jaringan yang hendak di akses oleh pengguna setelah mengubah alamat IP dari paket yang ditransmisikan oleh dua belah pihak. *Firewall* jenis ini bekerja pada lapisan *session layer*. Contoh ilustrasi *circuit level firewall* diperlihatkan pada gambar 2.12.



Gambar 2.12. Contoh Ilustrasi *Circuit Layer Firewall.*

Kelebihan *firewall* jenis ini antara lain lebih aman dibandingkan dengan jenis *packet filtering firewall* karena pengguna luar tidak dapat melihat alamat IP jaringan *internal* dalam paket-paket yang ia terima, melainkan alamat IP dari *firewall*. Protokol yang populer digunakan sebagai *Circuit-Level Gateway* adalah SOCKS v5.

2.2.6 *Virtual Private Network* (VPN)

VPN adalah singkatan dari *Virtual Private Network*, yaitu jaringan pribadi (lokal) yang menggunakan media nonpribadi (publik/*internet*) untuk menghubungkan antar *remote-site* secara aman. Perlu penerapan teknologi tertentu yang menggunakan media yang umum, tetapi *traffic* (lalu lintas) jalur data yang dikirim antar *remote-site* tidak dapat di-*snifing* (disadap) dengan mudah,

juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya. Beberapa keuntungan VPN antara lain:

1. *Anonymous surfing* (menjelajah internet tanpa terlacak).
2. Keamanan informasi yang diterima atau dikirim melalui internet dengan enkripsi *standar* VPN 128 bit / 1024 bit.
3. *Remote Access*, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet.
4. Melindungi komputer dari serangan *virus, malware, worm, trojan*, dsb.
5. Menjaga keamanan *User* dan *Password* dari *sniffers.*
6. Mempercepat koneksi yang terhubung dengan hotspot (dengan *bandwith limiter*).
7. Fleksibel Arsitektur, dapat dikoneksikan dengan infrastruktur yang sudah ada seperti peralatan *router/swtich* yang mendukung VPN.
8. Security, memungkinkan *traffic* kritikal bisnis dengan aman dengan digunakannya metode *tunneling* dan enkripsi.

Adapun beberapa kekurangan atau kelemahan VPN diantaranya adalah:

1. Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya “nebeng” koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
2. Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.
3. Perangkat tidak sesuai dikarenakan perangkat-perangkat pada VPN biasanya bersifat eklusif. Dalam artian adalah bisa dimungkinkan satu perangkat tidak bisa digantikan perangkat dengan merk berbeda. Sehingga dalam pembangunannya perlu memperhatikan jenis dan bahkan merk perangkat yang digunakan.

4. Tidak adanya standar yang memenuhi sebagai jaringan nirkabel, VPN dan banyak jenis yang lain, mengalami masalah ini, yaitu tidak adanya standar yang memenuhi. Antara satu pabrikan dengan pabrikan yang lain memiliki ketentuan masing-masing. Akibatnya perangkat tidak sesuai, termasuk akibat lain yang antara jaringan satu dengan yang lain tidak mampu berkomunikasi hanya karena perbedaan pada sisi perangkat.

2.2.6.1 Komponen Keamanan VPN

Untuk keamanan VPN terdiri dari 4 komponen, yaitu Autentikasi *User*, Kendali Akses, Enkripsi, dan *Public Key*, *Infrastructure* (PKI).

1. Autentikasi *User.*

Autentikasi adalah proses dalam rangka validasi *user* pada saat memasuki sistem. *Username* dan *password* dari pengguna diperiksa melalui proses yang memeriksa langsung daftar para *user,* yang diberikan hak untuk memasuki sistem.

2. Kendali Akses

Kendali akses (*acces control*) memliki kemampuan untuk memberikan akses (seperti hak terhadap *server*, direktori, dan *file*) yang berbeda kepada setiap *user* atau *group* tertentu dalam jaringan komputer lokal (*private network*) atau *remote access.*

3. Enkripsi

Enkripsi merupakan proses untuk mengubah, menyandikan atau mengkodekan sebuah pesan (informasi), sehingga tidak dapat dilihat atau dibaca tanpa menggunakan kunci pembuka.

4. *Public Key Infrastructure* (PKI)

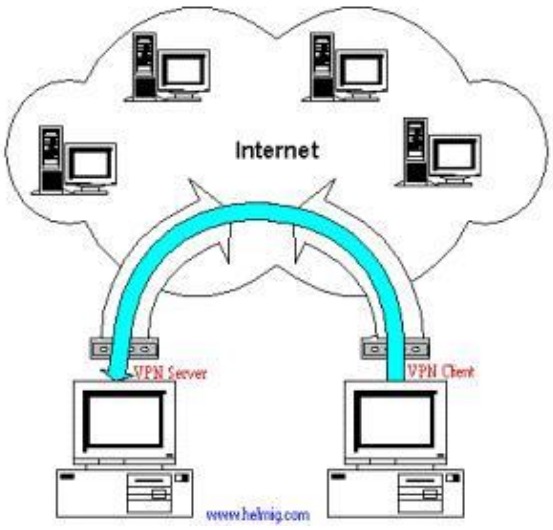
Public Key Infrastructure (PKI) adalah teknologi lanjutan, yang pada akhirnya menjadi standar IETF (*Internet Engineering Task Force*). Sasaran

PKI adalah menyediakan dasar untuk sistem yang akan mendukung berbagai layanan keamanan, sepeti integritas data, kerahasiaan data, dan autentikasi *user*.

2.2.6.2 Cara Kerja VPN

Dengan VPN ini seolah-olah membuat jaringan didalam jaringan atau biasa disebut *tunnel* (terowongan). *Tunneling* adalah suatu cara membuat jalur *private* dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi *tunneling* yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet *Protocol Security* (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi *tunneling* dan enkripsi.

Dibawah ini adalah gambaran tentang koneksi VPN yang menggunakan protokol PPTP. PPTP (*Pont to Point Tunneling Protocol*) adalah sebuah protokol yang mengizinkan hubungan *Point-to Point Protocol* (PPP) melewati jaringan IP, dengan membuat *Virtual Private Network* (VPN). Contoh ilustrasi VPN yang menggunakan protokol PPTP (*Pont to Point Tunneling Protocol*) diperlihatkan pada gambar 2.13.



Gambar 2.13. Contoh Ilustrasi VPN yang menggunakan protokol PPTP (*Pont to Point Tunneling Protocol*)

Cara kerja VPN (dengan protokol PPTP) adalah sebagai berikut:

1. VPN membutuhkan sebuah *server* yang berfungsi sebagai penghubung antar PC, *Server* VPN ini bisa berupa komputer dengan aplikasi VPN *Server* atau sebuah *Router*, misalnya MikroTik RB 750.
2. Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN *Client* mengontak *Server* VPN, VPN *Server* kemudian memverifikasi *username* dan *password* dan apabila berhasil maka VPN *Server* memberikan IP *Address* baru pada komputer *client* dan selanjutnya sebuah koneksi/*tunnel* akan terbentuk.
3. Untuk selanjutnya komputer *client* bisa digunakan untuk mengakses berbagai *resource* (komputer atau LAN) yang berada dibelakang VPN *Server* misalnya melakukan transfer data, *browsing* dengan *gateway* yang diberikan dari VPN *Server*, melakukan *remote desktop* dan lain sebagainya.

2.2.7 Spoofing

Serangan *spoofing* adalah situasi di mana satu orang atau program berhasil menyamar sebagai orang lain dengan memalsukan data, dengan demikian mendapatkan keuntungan secara tidak sah. Dalam jaringan komputer, alamat IP *spoofing* atau istilah IP *spoofing* mengacu pada penciptaan Internet (IP) Protokol paket dengan alamat IP sumber palsu, yang disebut *spoofing*, dengan tujuan menyembunyikan identitas pengirim atau meniru sistem komputasi lain.

2.2.8 SYN Flood

SYN Flood terjadi ketika *host* mengirimkan paket *SYN* secara besar-besaran, seringkali dengan alamat pengirim yang dipalsukan. Masing-masing paket ditangani seperti permintaan sambungan, menyebabkan *server* membangun sebuah koneksi yang setengah terbuka, dengan mengirimkan kembali TCP/SYN-ACK paket, dan menunggu paket dalam respon dari alamat pengirim (respons terhadap *Packet* ACK). Namun, karena alamat pengirim dipalsukan, tanggapan tidak pernah datang. Koneksi yang setengah terbuka ini membatasi kapasitas

jumlah koneksi yang dapat ditangani *server*, sehingga mencegah *server* menanggapi permintaan yang sah sampai serangan tersebut berakhir.

2.2.9 Metode *Prepare, Plan, Design, Implement, Operate, and Optimize* (PPDIOO) *Network Lifecycle*

Metode *Prepare, Plan, Design, Implement, Operate and Optimize* (PPDIOO) *Network Lifecycle* merupakan sebuah metode penelitian yang dikembangkan oleh *Cisco Systems* yang mendefinisikan sebuah siklus yang diperlukan dalam implementasi sebuah jaringan.

Siklus Hidup Jaringan Cisco atau disebut juga dengan metode *Prepare, Plan, Design, Implement, Operate and Optimize* (PPDIOO) *Network Lifecycle* adalah dirancang untuk mendukung jaringan yang sedang berkembang. Siklus Hidup Jaringan Cisco adalah pendekatan dengan enam tahap. Tiap tahap mendefinisikan aktifitas yang dibutuhkan untuk keberhasilan menyebarkan dan mengoperasikan teknologi Cisco. Hal ini juga terinci bagaimana mengoptimalkan kinerja di seluruh siklus hidup suatu jaringan.

Metode *Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle* yang terdiri dari beberapa tahap, yaitu:

a. *Prepare*

   Dalam model pengembangan sistem PPDIOO fase pertama dimulai dari *fase prepare*. Pada *fase* ini dilakukan proses perumusan masalah, mengidentifikasi konsep dari sistem yang akan diimplementasikan, jenis dan tipe penerapannya, serta komponen pendukung sehingga spesifikasi kebutuhan sistem dapat diperjelas.

b. *Planning*

   Untuk tahap selanjutnya adalah tahap *plan*. Penulis melakukan perencanaan dalam membuat rincian spesifikasi. Dalam penelitian ini terdapat perencanaan dalam membuat infrastruktur dan komponen pendukung yang akan dikonfigurasi.

c. *Design*

Dalam tahapan *design* ini dibuat suatu topologi jaringan untuk proses keamanan data. Serta konfigurasi yang dilakukan pada masing-masing perangkat.

d. *Implement*

Tahap selanjutnya adalah tahap implementasi, pada tahap ini menerapakan semua yang telah direcanakan. Dalam tahap ini mencakup instalasi serta konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat.

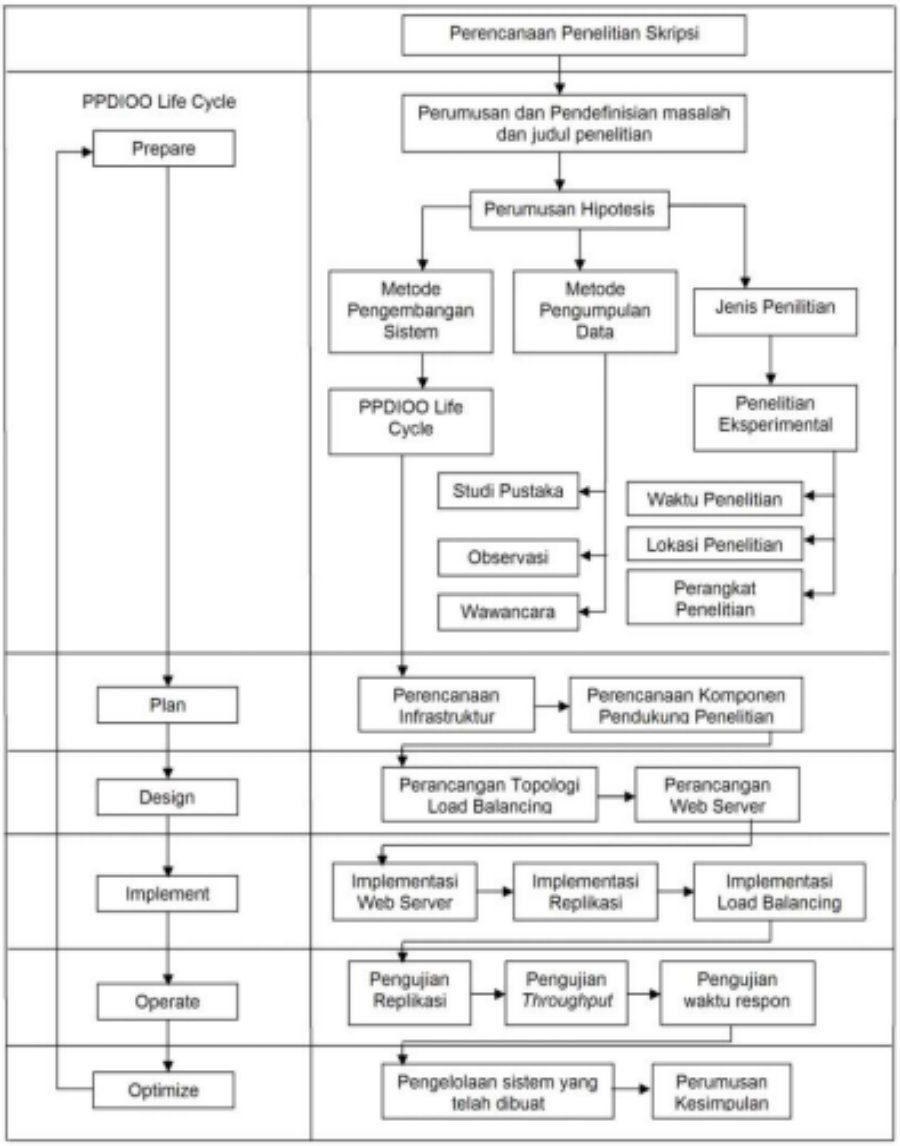
e. *Operate*

Dalam tahap ini diperlukan adanya pemantauan terhadap *server* agar berjalan sesuai dengan analisa awal dan pemantauan terhadap infrastruktur *hardware*. Proses pengujian termasuk dalam fase ini, dalam melakukan pengujian menggunakan parameter yang ditentukan dan sejumlah komponen pendukung agar dipastikan sudah berjalan dengan baik dan benar dan sudah menjawab permasalahan yang telah dirumuskan.

f. *Optimize*

Tahap ini memerlukan perhatian khusus terhadap kebijakan yang perlu dibuat untuk mengatur dan membuat sistem agar dapat berjalan dengan baik. Perawatan, pemeliharaan dan pengelolaan terhadap *server* termasuk dalam *fase* ini.

Contoh kerangka metode *Prepare, Plan, Design, Implement, Operate and Optimize* (PPDIOO) diperlihatkan pada gambar 2.14.



Gambar 2.14. Kerangka Metode *Prepare, Plan, Design, Implement, Operate and Optimize* (PPDIOO).