BAB 2
TINJAUAN PUSTAKA

2.1. Profile DPRD Provinsi Jawa Barat

Berikut ini adalah tinjauan umum profile singkat Lembaga Dewan Perwakiran Rakyat (DPRD) Provinsi Jawa Barat sebagai tempat penelitian, yaitu. [2]

2.1.1. Sejarah Singkat DPRD Provinsi Jawa Barat

Dalam tahun awal berdirinya Republik Indonesia, istilah DPRD Provinsi Jawa Barat belum digunakan. Meski demikian, hal ini tidak berarti bahwa tidak terdapat lembaga legislatif semacam DPRD. Pada tahun awal kemerdekaan lembaga semacam DPRD ini sesungguhnya telah juga hadir dengan nama Badan Perwakilan Rakyat Daerah (BPRD) Jawa Barat. Karena itu asal-usul dari kehadiran DPRD Provinsi Jawa Barat tidak dapat dipisahkan dari kehadiran BPRD Jawa Barat tersebut. Pada masa itu, BPRD dipimpin oleh R. Otto Iskandardinata dengan wakilnya Dr. Soeratman Erwin dan Mr. Samsudin.

2.1.2. Logo DPRD Provinsi Jawa Barat

Pada gambar 2.1 adalah logo resmi perusahaan yang digunakan oleh Dewan Perwakilan Rakyat (DPRD) Provinsi Jawa Barat.



Gambar 2. 1 Logo DPRD Provinsi Jabar

(*Sumber: dprd.jabarprov.go.id)*

2.1.3. Visi dan Misi

Sebagai lembaga yang berperan penting dalam pemerinatahan, Lembaga Dewan Perkawilan Rakyat Daerah memiliki visi dan misi, yaitu [2]:

2.1.3.1. Visi

Tingkatkan pelayanan informasi hukum secara tertib, terpadu dan berkesinambungan, mudah, capat serta akurat

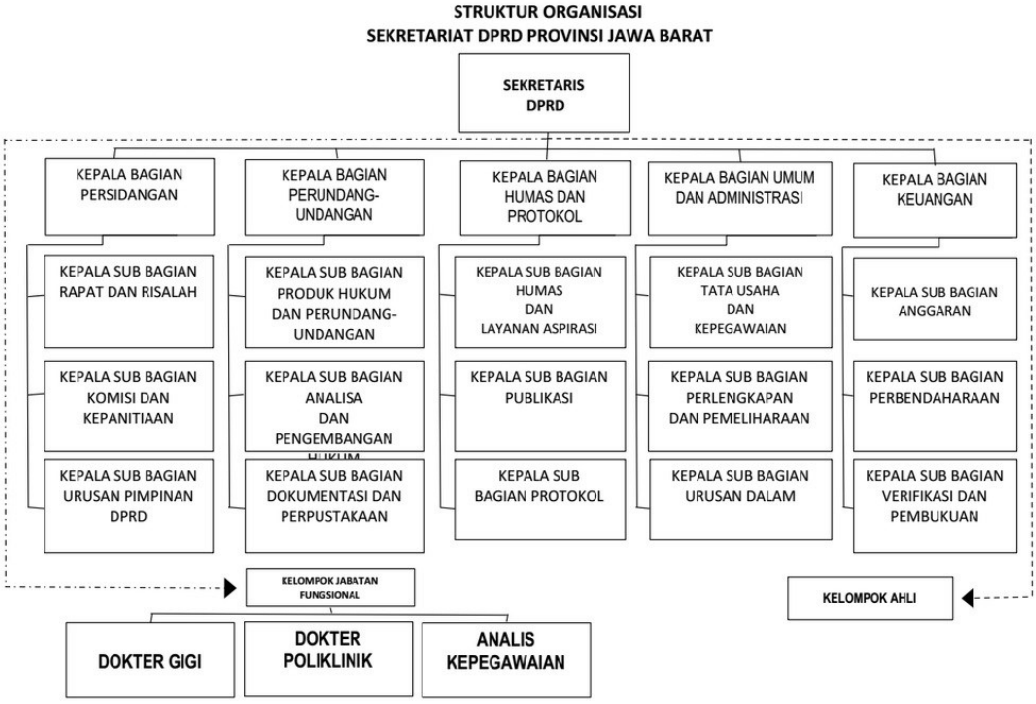
2.1.3.2. Misi

Sedangkn misi dari Dewan Perwakilan Rakyat Daerah (DPRD) Provinsi Jawa Barat ini adalah sebagai berikut:

1. Menyediakan sarana pembangunan bidang hukum dengan tertib, terpadu dan berkesinambungan.
2. Meningkatkan penyebarluasan dan pemahaman pengetahuan hukum.
3. Menyiapkan kemudahan pencarian dan penelusuran peraturan perundang-undangan dan bahan dokumentasi hukum lainnya.
4. Meningkatkan pemberian pelayanan pelaksanaan penegakan hukum dan kepastian hukum.
5. Penyediakan kemudahan akses informasi segala peraturan perundang-undangan yang tersedia dan dokumentasi hukum lainnya.

2.1.4. Struktur Organisasi

Berikut ini adalah struktur organisasi Dewan Perwakilan Rakyar Daerah Provinsi Jawa Barat beserta anggota dari masing – masing divisi.



Gambar 2. 2 Struktur Organisasi

(*Sumber: dprd.jabarprov.go.id)*

Berikut ini adalah nama – nama yang mengisi jabatan struktular pada Dewan Perwakilan Raktyat Daerah (DPRD) Provinsi Jawa Barat.

1. Sekretaris Dprd-Drs. H Daud Achmad
2. Kepala Bagian Persidangan-H. Eddy Setiawan, Sh. Mh.
3. Kepala Bagian Perundang-Undangan-Denny Yusuf, Sh., M. Si
4. Kepala Bagian Humas dan Protokol-Nanang Syaefudin, S. Sos, M. Si
5. Kepala Bagian Umum dan Administrasi-Dra.Hj. Siti Nina Nurasidah
6. Kepala Bagian Keuangan-Dra. Enny R Oetoyo, M. M

2.1.5. Deskripsi Kerja

Adapun deskripsi kerja masing – masing bagian adalah sebagai berikut ini.

2.1.5.1. Bagian Persidangan

Bagian Persidangan dan Risalah mempunyai tugas perumusan risalah atas penyelenggaraan rapat dan sidang Pimpinan dan Anggota DPRD sesuai dengan urusan yang menjadi kewenangan serta urusan lain untuk menunjang kebijakan Sekretaris DPRD dalam penyelenggaraan Pemerintahan. Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Bagian Persidangan dan Risalah mempunyai fungsi.

1. Penyiapan program persidangan dan risalah.
2. Penyiapan kegiatan rapat-rapat.
3. Penyiapan kebutuhan rapat-rapat.
4. Pembuatan Risalah, Notulen dan Catatan pada rapat-rapat.
5. Penghimpunan permasalahan-permasalahan yang timbul untuk dibahas dalam komisi dan rapat-rapat.
6. Pengkoordinasian kegiatan hearing/dialog dengan Pejabat Pemerintah dan Masyarakat.
7. Penyusunan program Triwulan pada rapat-rapat.
8. Pelaksanaan tugas lain yang diberikan atasan langsung.

2.1.5.2. Bagian Perundang – Undagan

Bagian Hukum dan Perundang-Undangan melaksanakan tugas dan fungsinya sesuai dengan urusan yang menjadi kewenangan serta urusan lain yang menunjang kebijakan Bupati dalam penyelenggaraan Pemerintahan. Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1) Bagian Hukum dan Perundang-Undangan mempunyai fungsi.

1. Penghimpunan dan pengumpulan peraturan perundang-undangan dan produk hukum daerah dan DPRD.
2. Pengelolaan perpustakaan Sekretariat DPRD.
3. Pelaksanaan fasilitasi bagi Anggota DPRD dalam penyusunan dan perencanaan Peraturan Daerah Inisiatif DPRD.

4. Pendataan, pengkajian dan evaluasi produk hukum daerah dan hukum DPRD;
5. Pembuatan konsep produk hukum DPRD terhadap keputusan DPRD dan keputusan Pimpinan DPRD.
6. Pendataan dan penginventarisasian produk hukum Daerah dan produk hukum DPRD.
7. Penyelenggaraan fasilitasi kegiatan s*OSI*alisasi Peraturan Perundang-Undangan oleh DPRD.
8. Penyampaian dan penyebar luasan informasi mengenai kegiatan DPRD kepada Media Cetak atau Elektronik atas persetujuan Pimpinan DPRD.
9. Penyelenggaraan fasilitasi Anggota DPRD dalam Peraturan Perundang-Undangan dan bahan mendasar lainnya dalam sidang-sidang dan rapat-rapat paripurna dan alat kelengkapan DPRD.
10. Pelaksanaan tugas-tugas lain yang diberikan oleh atasan sesuai lingkup bidang tugasnya.

2.1.5.3. Bagian Humas dan Protokol

Tugas Pokok bagian humas adalah melakukan pembinaan, koordinasi, monitoring dan evaluasi humas dan protokoler. Sedangkan fungsi pokoknya adalah sebagai berikut [4].

1. Merencana kegiatan sub bagian humas dan protokoler berdasarkan rencana kerja sekretariat DPRD sebagai pedoman dalam pelaksanaan tugas.
2. Membagi tugas tertentu dan memberikan petunjuk pelaksanaan tugas kepada bawahan sesuai ketentuan sehingga pelaksanaan tugas berjalan lancer.
3. Membimbing bawahan dalam rangka pelaksanaan tugas sesuai permasalahan yang timbul agar pelaksanaan tugas berjalan lancer.
4. Memeriksa hasil pelaksanaan tugas bawahaan sesuai peraturan dan prosedur agar diperoleh hasil kerja yang benar dan akutrat.
5. Menilai bawahaan sesuai pelaksanaan pekerjaan agar tercapai tingkat kinerja yang diharapkan.
6. Menyusun SOP berdasarkan peraturan perundang-undangan.

2.1.5.4. Bagian Umum dan Administrasi

Bagian Umum mempunyai tugas mengendalikan dan mengkoordinir administrasi perkantoran, administrasi kepegawaian dan administrasi keuangan serta urusan lain untuk menunjang kebijakan Bupati dalam penyelenggaran Pemerintahan. Bagian Umum mempunyai fungi.

1. Pengelolaan Tata Usaha, surar menyurat, administrasi perkantoran, administrasi kepegawaian dan administrasi keuangan.
2. Penyelenggaraan fasilitas perjalanan dinas.
3. Pengkoordiniran penyusunan dan pelaporan, perencanaan kegiatan Sekretariat DPRD.
4. Pengelolaan dan pengendalian dibidang arsip.
5. Pengendalian, ketertiban dan kebersihan kantor (K-3).
6. Penyelenggaran persiapan fasilitas rapat / persidangan.
7. Penyelenggaraan fungsi tehadap tugas lain yang diberikan atasan sesuai bidang lingkup tugasnya.

2.1.5.5. Bagian Keuangan

Bagian Keuangan dipimpin oleh Kepala Bagian berada di bawah dan bertanggung jawab kepada Sekretaris DPRD. Mempunyai tugas melaksanakan penyusunan anggaran, pertanggung-jawaban pelaporan keuangan DPRD dan Sekretariat DPRD. Adapaun fungsi bagian keuangan ini adalah sebagai berikut [4]:

1. Menyusun rencana anggaran DPRD dan Sekretariat DPRD dalam bentuk program, kegiatan dan rincian belanja.
2. Penyelenggaraan kegiatan penatausahaan keuangan DPRD dan Sekretariat DPRD.
3. Penyelenggaraan verifikasi bukti pertanggung-jawaban atas penggunaan keuangan DPRD dan Sekretariat DPRD.
4. Pengelolaan, pengendalian dan evaluasi administrasi keuangan serta pertanggung-jawaban keuangan DPRD dan Sekretariat DPRD.
5. Penyelenggaraan akuntansi DPRD dan Sekretariat DPRD.

6. Penyusunan laporan kegiatan di bidang tugasnya.
7. Pelaksanaan tugas lain yang diberikan pimpinan sesuai tugas da fungsinya.

2.2. Landasan Teori

Berikut ini adalah beberapa landasan teori yang digunakan oleh penulis sebagai pendukung teori dasar dari analisi dan implementasi system keamanan jaringan *menggunakan Unified Threat Management (UTM) Firewall* berbasis *Linux* di Dewan Perwakilan Rakyat Daerah (DPRD) Provinsi Jawa Barat.

2.2.1. Jaringan Komputer

Jaringan komputer adalah sekelompok komputer yang saling dihubungkan sehingga antara satu komputer dengan komputer yang lain dapat berbagi data atau berbagi sumber daya. Komputer - komputer yang terhubung dalam jaringan computer harus memakai aturan komunikasi yang sama. Hal ini dimaksudkan agar masing – masing komputer dapat berkomunikasi yang baik dengan komputer yang lainnya. Protokol yang menjadi *standar International* adalah *TCP/IP* (*Transmission Control Protocol / Internet Protocol*) [3].

2.2.1.1. *LAN*

Sebuah *LAN* adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi. Beberapa model konfigurasi *Local Area Network,* satu komputer biasanya di jadikan sebuah *file server*, yang mana digunakan untuk menyimpan perangkat lunak yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung ke dalam jaringan komputer [3].

2.2.1.2. *MAN*

Sebuah *Mertopolitan Area Network* biasanya meliputi area yang lebih besar dari *LAN*, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan - jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh misalnya DPRD se-Indonesia

yang ada di seluruh wilayah Indonesia di hubungkan pada pusat yaitu DPR yang berada di Jakarta.

2.2.1.3. *WAN*

Wide Area Network adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana satelit ataupun kabel bawah laut sebagai. *WAN* menggunakan banyak sarana untuk menghubungkan antara *Local Area Network* dan *Wide Area Neitwork* ke dalam Komunikasi *Global* seperti *Internet*. Klasifikasi jaringan komputer berdasarkan teknologi transmisinya jaringan dapat dibedakan menjadi:

1. Jaringan *Broadcast*

Jaringan *broadcast* memiliki saluran komunikasi tunggal yang dipakai bersamasama oleh semua mesin yang ada pada jaringan. Pesan-pesan berukuran kecil yang disebut paket, dikirimkan oleh suatu mesin dan akan diterima oleh mesin-mesin lainnya. *Field* alamat pada sebuah paket berisi keterangan tentang kepada siapa paket tersebut ditujukan. Saat menerima paket, mesin akan mengecek *field* alamat. Bila paket tersebut berisi alamat yang dituju sesuai maka mesin akan memproses paket data tersebut, bila tidak sesuai akan diabaikan saja. [3]

2. Jaringan *Point-to-Point*

Jaringan *Point-to-Point* terdiri dari beberapa koneksi pasangan individu dari mesinmesin. Untuk mengirim paket dari sumber satu ke sumber tujuan, sebuah paket pada jaringan mungkin harus melalui lebih dari satu mesin-mesin perantara, dan sering harus melalui rute yang jaraknya berbeda-beda sehingga pada jenis jaringan ini maka algoritma rute memegang peranan penting [3].

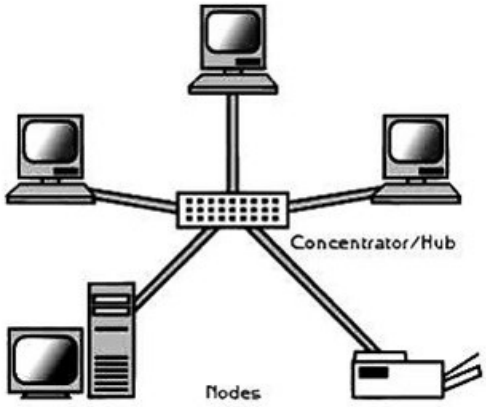
2.2.1.4 Tipe Jaringan Cilent – *Server*

Sistem operasi jaringan *client-server* memungkinkan jaringan untuk mensentralisasi fungsi dan aplikasi kepada satu atau dua *file server.* [3]

a. *single Server*
b. Dedicated Server

2.2.1.5. Topologi Jaringan

Topologi jaringan adalah peta dari sebuah jaringan. Topologi jaringan terbagi menjadi dua yaitu topologi secara fisik *(Physical Topology)* dan Topologi secara logika *(Logical Topology)*. Topologi secara fisik menjelaskan bagaimana susunan dari kabel dan komputer dan lokasi dari semua komponen jaringan. Sedangkan topologi secara logika menetapkan bagaimana informasi atau aliran data dalam jaringan [3]. *Switch* mendeteksi bila ada dua buah *workstation* yang akan saling berkomunikasi, kemudia *switch/hub* akan membuat jalur komunikasi virtual diantara kedua *workstation* tersebut sehingga data dapat terkirim melalui jalur tersebut seperti pada gambar 2.3.



Gambar 2. 3 Topologi *Star*

(Sumber: https://fcit.usf.edu/network/chap5/pics/star.gif)

2.2.1.6.Jaringan *Internet*

Internet merupakan dua komputer atau lebih yang saling berhubungan membentuk jaringan komputer hingga meliputi jutaan komputer di dunia, yang saling berinteraksi dan bertukar informasi, sedangkan dari segi ilmu pengetahuan, *Internet* merupakan sebuah perpustakaan besar yang didalamnya terdapat jutaan informasi atau data yang dapat berupa *teks, grafik, audio* maupun *animasi* dan lain lain dalam bentuk media elektronik [3].

2.2.1.7. Komponen Jaringan

Berikut ini adalah komponen – komponen standar dalam sebuah system jaringn komputer.

1. *Router*

Berfungsi untuk menerima *packet* dari pengirim untuk diteruskan ke stasiun penerima dan juga sebagai konversi *network* seperti pada gambar 2.4.



Gambar 2. 4 Router

(*Sumber: https://img.routerboard.com/mimg/832_l.jpg)*

2. *Switch*

Switch Sebuah alat yang menyaring dan melewatkan paket yang ada di sebuah *LAN*. *Switch* bekerja pada *layer data link* dan terkadang di *Network Layer* berdasarkan referensi *OSI Layer Model*.



Gambar 2. 5 *Switch*

(*Sumber: https://www.bhphotovideo.com /images2500x2500/cisco_sg112_24_.jpg)*

3. *Bridge*

Berfungsi untuk menghubungkan dua jaringan yang memiliki segmen yang sama seperti pada gambar 2.6.



Gambar 2. 6 *Bridge*

(*Sumberhttps://images.novatech.co.uk/netgear-gs105uk_extra1.jpg)*

Selain memperkuat sinyal seperti yang dilakukan repeater, *bridge* juga melakukan tranmisi ulang paket data dari satu segmen ke segmen yang lainnya.

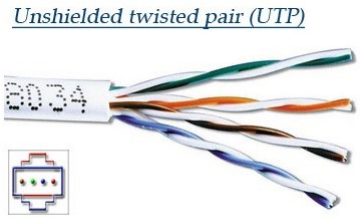
1.2.1.7.1. Media transmisi

Dalam menghubungkan komputer atau perangkat lainnya membutuhkan sebuah media transmisi. Media transmisi ini akan berfungsi sebagai jalur lintas data dan distribusi informasi. Secara garis besar penggunaan media untuk menghubungkannya terbagi atas beberapa yaitu:

1. Media Transmisi Kabel

a. Twisted Pair

Kabel ini memiliki dua jenis yaitu *Shielded Twisted Pair* (STP) dan *Unshielded Twisted Pair* (UTP). Perbedaan diantara keduanya adalah ada tidaknya lapisan pelindung interferensi. Kabel *UTP* merupakan kabel jaringan yang paling banyak digunakan karena kemudahan yang ditawarkan, yaitu kemudahan pengembangan jumlah *client* tanpa mengganggu sistem komunikasi. seperti pada gambar berikut ini.

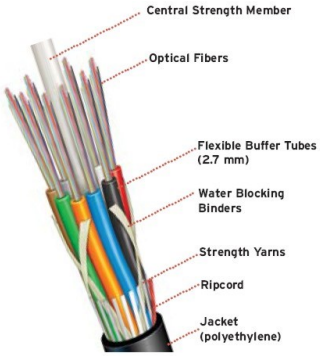


Gambar 2. 7 Kabel *UTP*

(*Sumber http://tech.dbagus.com/ Kabel-UTP.jpg)*

b. Serat Optik (*Fiber Optic*)

Serat optik menggunakan 2 buah ring. Pertama, *primary* ring yang digunakan untuk komunikasi data. Kedua, *secondary* ring yang digunakan sebagai media komunikasi cadangan. Kedua ring ini bertransmisi secara berlawanan (*counter rotating*) seperti pada gambar berikut ini.



Gambar 2. 8 Kabel *Fiber Optik*

(*Sumber http://4.bpt.com /s1600/konstruksi-1.jpg)*

2. Tanpa Kabel (*Wireless*)

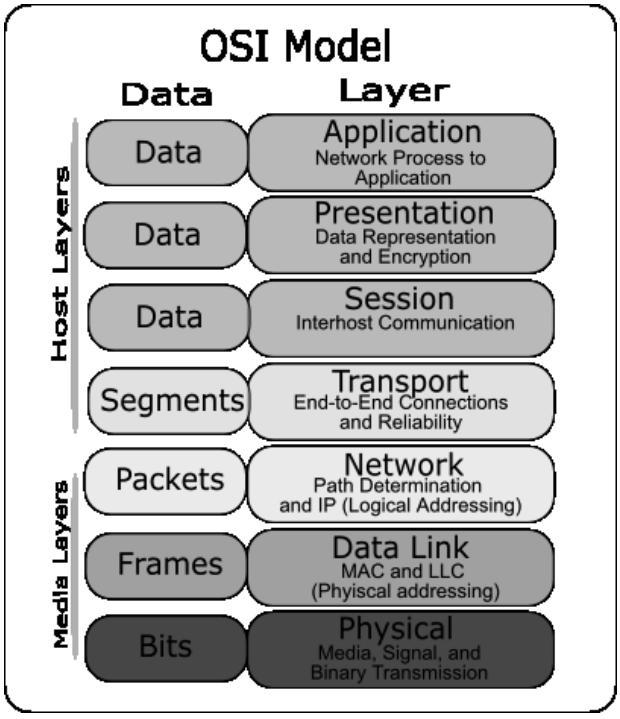
Wi-Fi merupakan singkatan dari *Wireless Fidelity* yang menggunakan standar *Institute of Electrical and Electronics Engineers* (*IEEE*) [6]. *Wi-Fi* merupakan suatu jaringan nirkabel yang menggunakan frekuensi radio untuk komunikasi antara perangkat dan akhirnya titik akses yang merupakan dasar dari *transiver* radio dua arah yang tipikalnya bekerja di *bandwith* 2,4 GHz (802.11b, 802.11g) atau 5 GHz (802.11a).

2.2.2. Lapisan Model *Layer OSI*

Model referensi jaringan terbuka *OSI* atau *OSI Reference Model for open networking* adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan *International Organization for Standardization* (ISO) di Eropa pada tahun 1977. Tidak adanya suatu protokol yang sama, membuat banyak perangkat tidak bisa saling berkomunikasi. Model referensi ini pada awalnya ditujukan sebagai basis untuk mengembangkan protokol-protokol jaringan, meski pada

kenyataannya inisatif ini mengalami kegagalan. Kegagalan itu disebabkan oleh beberapa faktor berikut: [3]

1. Standar model referensi ini, jika dibandingkan dengan model referensi *DARPA* (Model *Internet*) yang dikembangkan oleh *Internet Engineering Task Force* (IETF), sangat berdekatan. Model *DARPA* adalah model basis protokol *TCP/IP* yang populer digunakan.
2. Model referensi ini dianggap sangat kompleks. Beberapa fungsi (seperti halnya metode komunikasi *connectionless*) dianggap kurang bagus, sementara fungsi lainnya (seperti *flow control* dan koreksi kesalahan) diulang-ulang pada beberapa lapisan.
3. Pertumbuhan *Internet* dan protokol *TCP/IP* (sebuah protokol jaringan dunia nyata) membuat *OSI Reference Model* menjadi kurang diminati.



Gambar 2. 9 *Model Layar OSI*

(*Sumberhttps://fthmb.tqn.com/ about/Osi-model-.png)*

1. *Application layer*

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. *Presentation layer*

Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (redirector *software*), seperti layanan *Workstation* (dalam *Windows NT*) dan juga *Network shell* (semacam *Virtual Network Computing (VNC)* atau *Remote Desktop Protocol (RDP*).

3. *Session layer*

Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

4. *TransPort layer*

Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.

5. *Network layer*

Berfungsi untuk mendefinisikan alamat-alamat *IP*, membuat *header* untuk paket-paket dan kemudian melakukan routing melalui *Internet*working dengan menggunakan *router* dan *switch layer-3.*

6. *Data-link layer*

Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya Media *Access Control Address (MAC Address*)), dan menetukan bagaimana perangkatperangkat jaringan seperti *hub, bridge, repeater,* dan *switch layer 2* beroperasi. Spesifikasi *IEEE 802*, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control (LLC)* dan lapisan *Media Access Control (MAC).*

7. *Physical layer*

Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card (NIC)* dapat berinteraksi dengan media kabel atau radio.

2.2.3. Pengalamatan Jaringan *TCP*/IP

Metode pengalamatan pada layer aplikasi disediakan oleh *host*, metode penamaan ini mengizinkan *host* untuk dikonfigurasi dengan nama yang mudah diingat. Sistem pengalamatan ini yang dapat langsung dilihat oleh pengguna. Nomor *Port* merupakan metode pengalamatan yang disediakan di layer *host* to *host*. Nomor ini digunakan untuk mengambarkan *interface* dari *software* yang akan memproses pada sebuah *host*.

IP Address digunakan untuk metode pengalamatan layer *Internet*. Saat ini banyak digunakan *IP Versi 4*, menggunakan 32 bit biner dan sistem bilangan yang digunakan adalah bilangan desimal.

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

Tabel 2. 1 Tabel Metode *TCP/IP*

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

Diantara keempat metode pengalamatan di atas, metode pengalamatan *TCP/IP* yan sering digunakan yaitu *IP Address*. Setiap *device* yang terhubung ke jaringan *TCP/IP* membutuhkan paling sedikit satu *IP Address* yang bersifat unik,

tidak boleh ada dua atau lebih *IP Address* yang sama dalam satu jaringan. Sebuah alamat *IP Address* terdiri dari dua bagian, yaitu:

a. *Network ID*

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

b. *Host ID*

Host ID merupakan identitas bagi *host* (*workstation*, *server*, *interface router* dan device lain yang terhubung ke jaringan *TCP*/IP). Dari sisi penggunaanya, alamat *IP* terbagi dalam dua jenis, yakni:

c. *IP Private*

IP Address yang digunakan pada jaringan privat tidak digunakan pada jaringan publik. *IP Address* yang termasuk dalam kelas tersebut.

Tabel 2. 2 *IP Private*

Class	***IP Address***	***Subnet***		
A	1-126	1-255	1-255	1-255
B	127-191	1-255	1-255	1-255
C	192-254	1-255	1-255	1-255

d. IP Public

IP Address yang biasa digunakan pada jalur publik dan penggunaanya harus melalui proses registrasi dahulu. Alamat *IP* terbagi ke dalam lima kelas, yaitu A, B, C, D, dan E. Nilai pada oktet pertama menentukan kelas dari sebuah *IP Address*.

Tabel 2. 3 *IP Public*

Class	***IP Address***	***Subnet***		
A	1-126	1-255	1-255	1-255
B	127-191	1-255	1-255	1-255

C	192-223	1-255	1-255	1-255
D	224-239	1-255	1-255	1-255
E	240-255	1-255	1-255	1-255

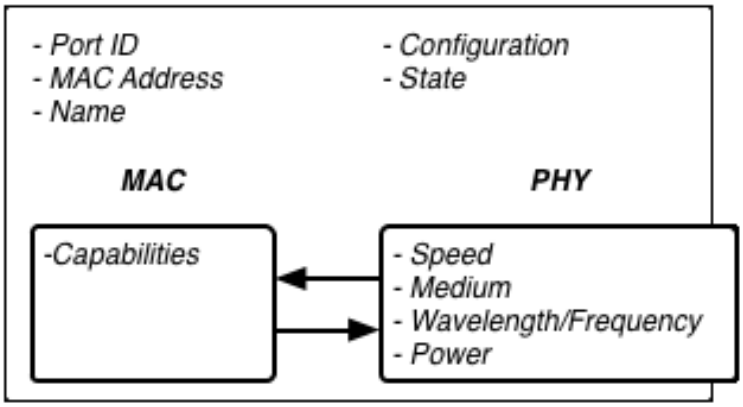
2.2.4. *Port* Jaringan Komputer

Port fisik adalah *Port* yang ketahui secara luas. *Port* fisik dapat dilihat dan rasakan secara fisik. Fungsi utama dari *Port* fisik ini pun untuk melakukan penghubungan dua atau lebih komponen yang nyata secara fisik, misalnya menghubungkan antara komputer dengan *server* dengan kabel, ataupun perangkat lainnya.

Port logic. berbeda dengan *Port* fisik, *Port* logic merupakan jenis *Port* yang tidak dapat terlihat secara fisik, dan tidak dapat dipegang atau raba. Tetapi *Port* logic ini juga memiliki fungsi yang sama untuk saling menghubungkan antar perangkat melalui protocol ataupun melalui media lainnya [3].

2.2.5. *Port* yang Digunakan pada Jaringan Komputer

Pada sebuah jaringan komputer, baik *Port* fisik maupun *Port* logic, keduanya merupakan jenis *Port* yang digunakan secara bersamaan. Fungsi dari kedua *Port* ini saling berhubungan. Dimana apabila tidak ada salah satu *Port*, maka hubungan dari sebuah jaringan tidak akan dapat terbangun [4].



Gambar 2. 10 *Port Logic dan Physic*

(*Sumberhttp://mvn.edu.in/lms/pluginfile.php/109/mod_book/chapter/17/a3.png)*

a. *Port* Fisik pada Jaringan Komputer

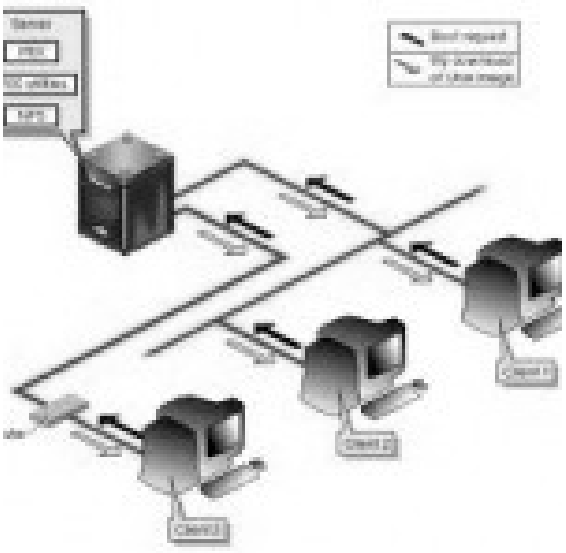
Apabila diperhatikan secara fisik, maka *Port* yang digunakan pada sebuah jaringan komputer adalah *Port* pada *Ethernet* atau *LAN Card*. *Port* fisik ini bertugas untuk membantu kabel agar dapat terhubung dengan jaringan, ataupun terhubung dengan perangkat jaringan yang lainnya.

b. *Port* Logik pada Jaringan Komputer

Secara umum ada banyak *Port* logic yang digunakan dalam sebuah jaringan, baik itu jaringan LAN, *Internet*, *WAN*, jaringan yang menggunakan protocol tertentu dan sebagainya. Pada dasarnya sebuah *Port Logic* pada jaringan komputer dan juga pada sebuah komputer terdiri dari banyak sekali jenis dan fungsinya. Apabila diurutkan secara runtut, sebuah *Port* logic di dalam komputer dan jaringannya terdiri dari *Port* 0 hingga *Port* 10000.

2.2.6. Protokol Jaringan

Pengertian Protokol Jaringan adalah satu set aturan yang mengatur online komunikasi di antara beberapa buah komputer yang ada dalam suatu jaringan. Peraturan-peraturan tersebut termasuk pedoman yang mencakup beberapa kriteria-kriteria sebuah jaringan. Ini termasuk cara mengakses, topologi fisik yang diizinkan, jenis-jenis perkabelan, dan kecepatan pengiriman data. Protokol Jaringan diibaratkan sebagai bahasa komunikasi antar komputer dalam jaringan [4].



Gambar 2. 11 Protokol Jaringan

(*Sumber https://protokoljaringan.com/2013/12/protokol-jaringan2.jpg)*

1. **Protokol Jaringan *Ethernet***

Protokol Jaringan *Ethernet* merupakan protokol yang paling banyak digunakan. *Ethernet* menggunakan cara masuknya (access method) yang dikenal sebagai *CSMA / CD (Carrier Sense Multiple Access / Collision Detection).* Protokol Jaringan *Ethernet* biasanya digunakan untuk topologi *linear bus, star* atau *tree*. Data bisa dikirim menggunakan kabel pasangan berpintal (*twisted pair)*, kabel sipaksi *(coaxial)* atau kabel *fiber optik* pada kecepatan 10 *Mbps.*

2. **Protokol Jaringan *Fast Ethernet***

Untuk meningkatkan pengiriman informasi yang lebih cepat, protokol *Ethernet* telah membangun suatu standar yang mendukung dan memungkinkan 100 *Mbs*. Inilah yang dikenal sebagai *Ethernet* pantas. *Ethernet* cepat membutuhkan penggunaan concentrator atau pusat yang berbeda dan lebih mahal biayanya dan jaringan kartu antarmuka *(network interface card).* Sebagai tambahan, kabel 5 pasangan berpintal *(twisted pair)* atau kabel *fiber optik* jika perlu.

3. **Protokol Jaringan *Local Talk***

Local Talk adalah protokol jaringanyang dikembangkan oleh *Apple Computer* untuk Komputer *Macintosh*. Cara yang digunakan oleh *Local Talk*

disebut *CSMA / CA (Carrier Sense Multiple Access dengan Collision Avoidance).* Ia hampir sama dengan *CSMA / CD* kecuali komputer memberi sinyal sebelum data akan dikirim. Adapter untuk *Local Talk* dan kabel pasangan berpintal yang khusus bisa digunakan untuk menghubungkan satu seri komputer menggunakan *Port* bersiri. Sistem operasi Macintosh memungkinkan sitem operasi sesama *client (peer-to-peer)* tanpa perlu perangkat lunak tambahan. Dengan penambahan versi *file server* dari perangkat lunak *AppleShare*, sistem klien-*server* (*client-server*) boleh dilaksanakan.

4. Protokol *Local Talk*

Mengizinkan topologi linear bus atau topologi tree dengan menggunakan kabel pasangan berpintal. Satu kekurangan kecil untuk *Local Talk* adalah dari segi kecepatan. Kecepatan untuk pengiriman informasi untuk *Local Talk* hanya 230 *Kbps.*

5. Protokol Jaringan Token *Ring*

Di dalam *Token Ring*, beberapa komputer dihubungkan untuk memungkinkan sinyal tinggal di sepanjang online jaringan komputer tersebut. Satu *Token* elektronik bergerak mengelilingi lingkaran dari satu komputer ke satu komputer dan jika komputer tersebut tidak memiliki informasi untuk dikirim, ia akan bergerak melewati komputer tersebut ke stasiun kerja berikutnya. Jika komputer tersebut akan mengirimkan informasi, ia akan mengisi data atau informasi kepada *Token* yang datang kepadanya.

6. Protokol Jaringan *Fiber Distributed Data Interface* (*FDDI*)

satu protokol jaringan terutama untuk menghubungkan dua atau lebih jaringan area lokal, untuk meliputi wilayah yang jauh jaraknya. Pengiriman biasanya terjadi pada salah satu dari *Token* atau Ring, namun begitu jika terjadi kegagalan di dalam jaringan, sistem tersebut akan menggerakkan informasi secara otomatis menggunakan perjalanan jaringan yang kedua menciptakan satu jaringan baru yang lengkap.

7. *TCP/IP* (*Transmission Control Protocol/Internet Protocol*)

TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas *Internet* dalam proses tukar-menukar data dari satu komputer ke komputer lain di

dalam jaringan *Internet*. *TCP*/*IP* mengimplemenasikan arsitektur berlapis yang terdiri atas empat lapis, diantaranya adalah:

a. Protokol lapisan aplikasi
b. Protokol lapisan antar-*host*
c. Protokol lapisan *Internetwork*
d. Protokol lapisan antarmuka jaringan

8. *UDP* (*User Datagram Protokol*)

UDP, singkatan dari *User Datagram Protocol*, adalah salah satu protokol lapisan transpor *TCP*/*IP* yang mendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi (*connectionless*) antara *host-host* dalam jaringan yang menggunakan *TCP*/*IP*.

9. *Domain Name System* (*DNS)*

Domain Name System (DNS) adalah *distribute database system* yang digunakan untuk pencarian nama komputer *(name resolution*) di jaringan yang mengunakan *TCP/IP (Transmission Control Protocol/Internet Protocol)*. *DNS* biasa digunakan pada aplikasi yang terhubung ke *Internet* seperti *Web browser* atau *email*, dimana *DNS* membantu memetakan *host* name sebuah komputer ke *IP Address*.

10. *Point-to-Point* Protocol

Point-to-Point Protocol (sering disingkat menjadi *PPP*) adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada *wide area network (WAN).*

11. *Serial Line Internet Protocol*

Serial Line Internet Protocol dianggap berkaitan erat dengan pengertian berikut Disingkat dengan *SLIP*. Sebuah protokol yang memungkinkan pemindahan data *IP* melalui saluran telepon. Alat bantu lainnya dalam *SLIP* adalah *PPP* yang mendeteksi kesalahan dan konfigurasi.

12. *Internet Control Message Protocol (ICMP)*

ICMP adalah salah satu protokol inti dari keluarga. *ICMP* berbeda tujuan dengan *TCP* dan *UDP* dalam hal *ICMP* tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. Salah satu pengecualian adalah aplikasi ping

yang mengirim pesan *ICMP Echo Request* (dan menerima *Echo Reply*) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan *protokol Internet*. *ICMP* utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

13. *POP3 (Post Office Protocol)*

POP3 adalah kepanjangan dari *Post Office Protocol* version 3, yakni protokol yang digunakan untuk mengambil *email* dari *email server*. Protokol *POP3* dibuat karena desain dari sistem *email* yang mengharuskan adanya *email server* yang menampung *email* untuk sementara sampai *email* tersebut diambil oleh penerima yang berhak. Kehadiran *email server* ini disebabkan kenyataan hanya sebagian kecil dari komputer penerima *email* yang terus-menerus melakukan koneksi ke jaringan *Internet*.

14. *IMAP (Internet Message Access Protocol)*

IMAP (*Internet Message Access Protocol*) adalah protokol standar untuk mengakses/mengambil *email* dari *server*. *IMAP* memungkinkan pengguna memilih pesan *email* yang akan ia ambil, membuat folder di *server*, mencari pesan *email* tertentu, bahkan menghapus pesan *email* yang ada.

15. *HTTP (Hypertext Transfer Protocol)*

HTTP (Hypertext Transfer Protocol) suatu protokol yang digunakan oleh *WWW (World Wide Web). HTTP* mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari *server* ke *client*. *HTTP* juga mengatur aksi-aksi apa saja yang harus dilakukan oleh *Web server* dan juga *Web* browser sebagai respon.

16. *HTTPS*

Https adalah versi aman dari *HTTP*, protokol komunikasi dari *World Wide Web.* Ditemukan oleh *Netscape Communications Corporation* untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris. Selain menggunakan komunikasi *plain text, HTTPS* menyandikan data sesi menggunakan protokol *SSL (Secure Socket layer)* atau protokol *TLS (TransPort Layer Security).* Kedua protokol tersebut memberikan perlindungan yang

memadai dari ancaman serangan *eavesdroppers*, dan *man in the middle attacks*. Pada umumnya *Port HTTPS* adalah 443.

17. *SSH (Secure Shell)*

SSH adalah protocol jaringan yang memungkinkan pertukaran data secara aman antara dua komputer. *SSH,* dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim *file* membuat *Tunnel* yang terenkripsi. Protocol ini mempunyai kelebihan disbanding protocol yang sejenis seperti *Telnet, FTP*, *Danrsh*, karena *SSH* memiliki system Otentikasi, Otorisasi, dan enkripsinya sendiri. Dengan begitu keamanan sebuah sesi komunikasi melalui bantuan *SSH* ini menjadi lebih terjamin.

18. *Telnet* (*Telecommunication Network*)

Telnet adalah sebuah protokol jaringan yang digunakan di koneksi *Internet* atau *Local Area Network*. *TELNET* dikembangkan pada 1969 dan distandarisasi sebagai *IETF STD 8*, salah satu standar *Internet* pertama. *TELNET* memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

19. *FTP* (File Transfer Protocol)

FTP (File Transfer Protocol) adalah sebuah protocol *Internet* yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) computer antar mesin-mesin dalam sebuah *Internetwork*.

20. *LDAP*

LDAP (Lightweight Directory Access Protocol) adalah protokol perangkat lunak untuk memungkinkan semua orang mencari resource organisasi, perorangan dan lainnya, seperti file atau printer di dalam jaringan baik di *Internet* atau intranet.

21. *SSL (Secure Socket Layer)*

SSL (Secure Socket Layer) adalah *arguably Internet* yang paling banyak digunakan untuk enkripsi. Ditambah lagi, *SSL* digunakan tidak hanya keamanan koneksi *Web*, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan *end-to-end*. *Secure Sockets Layer* (*SSL*) merupakan sistem yang digunakan untuk enkripsi pengiriman informasi pada *Internet*, sehingga data dapat dikirim dengan aman.

2.2.7. Keamanan Jaringan Komputer

Keamanan jaringan komputer tindakan pencegahan dari ancaman serangan pengguna jaringan komputer atau pengakses jaringan yang tidak bertanggung jawab [10].

2.2.6.1. Aspek keamanan jaringan

Secara umum keamanan komputer terdiri dari empat aspek, yaitu *privacy, Integrity, Authetincation, Availability* dan *access control* [5].

1. Privacy/Confidentiality

Keaman *Privacy/Confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* (kerahasiaan) lebih kearah data-data yang sifatnya *private*, contoh dari privacy adalah *email* atau *file-file* user yang tidak boleh dibaca orang lain meskipun oleh administrator.

2. Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat informasi di kirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirimkan dengan yang diterima maka aspek *integrity* tidak tercapai. Adanya *virus, Trojan horse*, atau pemakai lain yang mengubah informasi tanpa izin merupakan salah satu contoh masalah yang harus dihadapi.

3. Authentication

Kunci aspek ini berhubungan dengan metode atau cara yang menyatakan bahwa informasi tersebut betul-betul asli, user yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang telah hubungi adalah betul-betul *server* asli.

4. Availability

Aspek ini berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Aspek ini berhubungan dengan ketersediaan data ketika dibutuhkan.

5. *Access Control*

Aspek ini berhubungan dengan *policy* atau aturan yang ada pada suatu jaringan komputer. Intinya ada suatu mekanisme yang mengatur siapa saja yang boleh melakukan aktivitas didalam jaringan tersebut. Hal ini biasanya berhubungan dengan klasifikasi data *(public, private, confidential, top secret)* dan *user (guest, admin)* mekanisme *Authentication* dan juga *privacy*. *Access control* seringkali dilakukan dengan menggunakan kombinasi *userid* atau *password* dengan menggunakan mekanisme lain (seperti kartu).

2.2.6.2. Aspek ancaman keamanan

Aspek-aspek ancaman keamanan komputer dalam dunia *Cyber* yang sangat keras saat ini, ancaman akan keamanan komputer sudah sangat memilikin resiko yang tinggi. Banyaknya orang yang sudah memilkin kemampuan untuk melakukan penerobosan dalam sistem keamanan pada komputer sehingga mereka bisa mengetahui celah yang bisa dilalui untuk mendapatkan informasi atau data yang diinginkan oleh pelaku kejahatan *cyber* [5].

1. *Interruption*

Interruption merupakan ancaman terhadap *availability*. Informasi dan data yang ada dalam sistem komputer dirusak dan dihapus, sehingga jika dibutuhkan, data atau informasi sudah tidak ada lagi.

2. *Interception*

Interception merupakan ancaman terhadap kerahasiaan. Informasi yang ada disadap atau orang yang tidak berhak untuk mendapatkan akses ke komputer di mana informasi tersebut disimpan. Pada aspek ini, data berhasil diambil sebelum atau sesudah data ditransmisikan ke tujuan. Teknik ini sangat sering dilakukan dan sangat transparan.

3. Modifikasi

Aspek modifikasi merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan tersebut. Pada Aspek ini informasi atau data tidak langsung terkirim ke tujuan, namun terkirim ke pelaku dan pelaku mempunyai otoritas full

apakah data ingin diubah, dihapus bahkan pelaku bisa saja tidak meneruskan informasi tersebut ke tujuan.

4. *Fabrication*

Fabrication merupakan ancaman terhadap integrity. orang yang tidak berhak berhasil meniru dengan memalsukan suatu informasi yang ada sehingga orang menerima informasitersebut, menyangka informasi tersebut berasal dari orang yang dikehendaki informasi tersebut.

2.2.6.3. Ancaman serangan Sistem Komputer

Ancaman serangan pada suatu sistem jaringan komputer sendiri pada dasarnya memiliki tiga gelombang utama yaitu [6].

1. Gelombang pertama adalah ancaman serangan fisik. Ancaman serangan ini ditujukan kepada fasilitas jaringan, perangkat elektronik, dan komputer.
2. Gelombang kedua adalah ancaman serangan sintaktik. Ancaman serangan ini ditujukan terhadap kerentanan *(vulnerability)* pada *software*, celah yang ada pada algoritma kriptografi atau protokol.
3. Gelombang ketiga adalah ancaman serangan semantik. Ancaman serangan jenis ini memanfaatkan arti dari isi pesan yang dikirim.

2.2.6.4. Masalah – masalah keamanan

Adapun masalah – masalah dalam hal keamanan jaringan adalah sebagai berikut [6].

1. Kehilangan data (*Data Losses*):

a. Bencana seperti kebakaran, banjir, gempa bumi, perang, kerusuhan, gangguan binatang.
b. Kesalahan perangkat (Lunak dan Keras) seperti *bugs*, saluran komunikasi, pemrosesan tidak berfungsi, media penyimpanan yang rusak
c. Kelalaian manusia seperti *input data*, pemasangan media penyimpanan yang salah, eksekusi program salah, kehilangan media penyimpanan

2. Penyusupan (*Intruder*):

a. Penyusup pasif, membaca data yang tak diotorisasi
b. Penyusup aktif, mengubah data yang tak diotorisasi Kategori Penyusupan:

1) Non-Teknis pada saat input data atau password
2) Penyadapan oleh orang dalam
3) *Penyerang* untuk berbagai macam tujuan
4) *Intelejen* (*Spionase* militer atau bisnis)

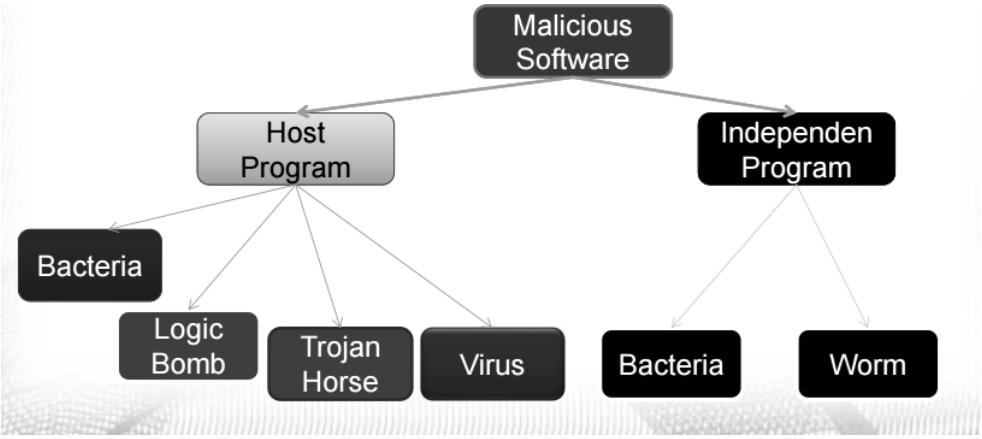
2.2.6.5. Ancaman serangan Sistem Jaringan Komputer

Sniffer *Device* yang dapat memonitor proses yang sedang berlangsung sebagai berikut [6].

1. *Spoofing* Penggunaan komputer untuk meniru atau dengan cara menimpa identitas *IP Address*.
2. *Remote Attack* Segala bentuk ancaman serangan terhadap suatu sistem/komputer dimana penyerangnya memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh diluar sistem jaringan atau media transmisi.
3. *Hole* Kondisi dari *software* atau *hardware* yang bisa diakses oleh pemakai yang tidak memiliki hak / otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi *Phreaking* Perilaku menjadikan sistem pengamanan telepon melemah.
4. *Penyerang* Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya. *Penyerang* tidak merusak sistem.
5. *Craker* Orang yang secara diam-diam mempelajari sistem dengan maksud jahat Muncul karena sifat dasar manusia yang selalu ingin membangun.

2.2.6.6. Ancaman Prangkat Lunak (*Malicius Program*)

Program yang memerlukan *host* dimana program ini tidak dapat mandiri secara independen dari suatu program aplikasi, utilititas atau program sistem. Program yang tidak memerlukan *host*, yaitu program yang dapat dijadwalkan dan dijalankan oleh sistem operasi [7].



Gambar 2. 12 Jenis *Malicious*

(*Sumber https://protokoljaringan.com/2013/12/protokol-jaringan2.jpg)*

2.2.6.6.1. Virus

Sebuah program yang dirancang untuk menyebarkan diri ke program atau menginfeksi *file* lain, sistem, *harddisk, floppy disk, flash disk*, dengan melakukan perubahan atau penghancuran *file* atau menyebabkan sistem menjadi crash. Sebuah komputer terinfeksi virus apabila terjadi pemanggilan/pembukaan program atau *file* bervirus oleh sistem. Saat program atau *file* bervirus dipanggil atau dibuka, maka virus akan mengambil satu atau lebih segmen di dalam memori untuk melakukan penyebaran. Empat langkah kerja virus yaitu. [7]

1. Development, Tahap penetrasi.
2. Tahap propagation.
3. Tahap triggering.
4. Tahap Damage.

2.2.6.6.2. Trojan horse

Trojan horse datang dengan kejutan tersembunyi yang diharapkan oleh programmernya tetapi secara total tidak diduga oleh pengguna komputer. Dirancang untuk membuat kerusakan atau keanehan pada sistem komputer tetapi disamarkan, seolah-olah semuanya bekerja normal. Berbeda dengan virus, *Trojan horse* tidak melakukan penyebaran diri, tetapi *Trojan horse* dapat menyebabkan kerusakan yang serius pada sebuah komputer [7].

2.2.6.6.3. Worm

Tidak menyebarkan diri dari satu *file* ke *file* lainnya, tetapi worm menyebarkan diri untuk menginfek dari satu komputer ke komputer yang lain. Dirancang untuk melakukan infeksi melalui medium jaringan seperti *TCP/IP*, *Email*, dan lain-lain. Worm lebih tertarik menginfeksi komputer dalam jaringan sebanyak-banyaknya dari pada menginfeksi *file-file* pada sebuah komputer. Sekali *worm* menginfeksi sebuah sistem, worm akan melakukan penyebaran diri untuk menginfeksi sistem lain yang ada dalam sebuah jaringan [7].

2.2.6.6.4. Hoax

Sebuah *email* yang berisi provokasi untuk meyakinkan bahwa tidak ada ancaman virus, atau menakut-nakuti agar *email* tersebut di-*forward* ke orang lain. Proses forward ini akan menyababkan jaringan mengalami *traffic* yang tinggi, sehingga sistem jaringan bisa terganggu. Hal ini akan sangat terasa apabila semakin banyak orang melakukan *forwarding email*, apalagi dalam lingkungan jaringan yang besar [7].

2.2.6.6.5. Spywar

Komponen aplikasi yang tersembunyi yang umumnya terdapat pada program-program *freeware* (demo) atau *shareware*. Sekali *spyware* terinstal pada komputer, maka *spyware* akan melakukan monitor aktifitas pengguna komputer secara *underground* (tanpa diketahui pengguna). *Spyware* bekerja mulai dari sekedar menampilkan pesan-pesan promosi melalui *Internet* hingga pengumpulan informasi-informasi yang ada dalam *system* [7].

2.2.6.6.6. *Malware*

Malware kependekan dari *Malicious Software* adalah sebuah istilah yang mencakup beberapa program yang dirancang untuk menyerang, menurunkan, dan menghambat kinerja sistem atau jaringan. *Malware* bisa berupa *virus, Trojan, worm, malicious active content,* atau *danial of service attacks (DOS).* Kasus invasi pribadi untuk kepentingan penipuan atau pencurian identitas melalui *software* yang disisipkan pada sebuah sistem juga termasuk *malware* [7].

2.2.6.6.7. Adware

Adware memberikan pesan iklan yang memungkinkan lebih sesuai dengan yang diharapkan. *Adware* juga merupakan komponen aplikasi yang tersembunyi dari program *freeware* (demo) atau *shareware*. *Adware* yang sudah terinstal dalam sistem biasanya akan bekerja saat program utamanya dijalankan.

2.2.6.7. Ancaman serangan Sistem Jaringan Komputer

Berikut ini adalah beberapa port dalam sebuah sistem komputer jaringan yaitu [7].

1. *Port* Scanning dilakukan sebagai tahap awal sebuah ancaman serangan. Untuk dapat melakukan penyerangan, seorang *cracker* perlu mengetahui aplikasi apa saja yang berjalan dan siap menerima koneksi dari lokasinya berada.
2. *DOS/DDOS (Denial of Services dan Distributed Denial of Services) adalah* ancaman serangan yang bertujuan untuk menghabiskan sumber daya sebuah *device* jaringan komputer sehingga layanan jaringan komputer menjadi terganggu
3. *Packet Sniffing* ancaman serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket didapat, kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.
4. *IP Spoofing* dan *DNS Forgery* ancaman serangan yang bertujuan untuk menipu seseorang. Dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan *Firewall* dan menipu *host* penerima data

2.2.6.8. Sistem keamanan Jaringan Komputer

Berikut ini adalah macam – macam sistem keamanan yang digunakan untuk dalam hal keamanan sistem jaringan komputer, yaitu [7].

1. *Intrusion Detection System (IDS)* dan *Intrusion Prevention System (IPS*) adalah sistem yang banyak digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari ancaman serangan oleh pihak luar maupun dalam.

2. *Network Topology*, Pembagian kelompok komputer sesuai dengan tugas dan fungsinya.
3. *Port Scanning*, Aplikasi yang memeriksa *Port* yang terbuka yang menunjukkan adanya aplikasi jaringan komputer yang siap menerima koneksi. Aplikasi ini dapat menjadi pintu masuk penyerang ke dalam sistem jaringan komputer.
4. *Packet Finger Printing*, sebuah *device finger printing* akan melihat bagaimana *device* jaringan komputer atau sistem operasi yang bersangkutan memberikan nilai-nilai awal pada beberapa bagian di *header IP*.
5. *Security Information Management,* berfungsi untuk menyediakan seluruh infomasi yang terkait dengan pengamanan jaringan komputer secara terpusat.
6. *Firewall* berfungsi sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *Firewall* mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan *private* yang dilindungi, beberapa kriteria yang dilakukan *Firewall* untuk memperbolehkan paket data lewati atau tidak.
7. *Anti-Virus* sebuah jenis perangkat lunak yang digunakan untuk mengamankan, mendeteksi, dan menghapus virus komputer dari sistem komputer. *Antivirus* disebut juga perangkat lunak perlindungan virus. Program ini dapat menentukan apakah sebuah sistem komputer telah terinfeksi dengan sebuah virus atau tidak.
8. *Anti-Spam* sebuah jenis perangkat lunak yang digunakan untuk mengamankan *email server* atau account *email* dari *spam.*
9. *VPN* adalah singkatan dari *Virtual Private Network*, yaitu jaringan pribadi yang menggunakan medium non-pribadi misalnya *internet* untuk menghubungkan antar *remote-site* secara aman.
10. *Content Filtering* sebuah jenis sistem keamanan yang digunakan untuk menyaring semua *content* yang bisa diakses atau tidak.

2.2.6.9. Lapisan keamanan jaringan

Berikut ini adalah lapisan – lapisan dalam keamanan sistem komputer jaringan yaitu [7].

1. Lapisan Fisik
2. Keamanan *local*
3. Keamanan *Root*
4. Keamanan *File* dan system *file*
5. Keamanan Password dan enkripsi
6. Keamanan *Kernel*
7. Keamanan Jaringan

2.2.6.10. Transite Keamanan Jaringan

Secara umum ada dua metode pada sistem keamanan jaringan komputer, yaitu [7].

1. Metode yang digunakan untuk melindungi data saat transit jaringan
2. Metode kontrol paket yang transit ke jaringan

Sementara kedua metode ini secara drastis mempengaruhi *traffic* yang ke dan dari sebuah situs, namun tujuannya sangat berbeda.

2.2.7. Firewall

Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap hardware*, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, *server*, *router,* atau *LAN* [7].

2.2.7.1. Karakteristik *Firewall*

Berikut adalah beberapa karakteristik – karekristik dari *Firewall*, yaitu.

1. Seluruh kegiatan dari dalam ke luar, harus melewati *Firewall*. Hal ini dapat dilakukan dengan cara memblok atau membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati *firewall*. Banyak sekali bentuk jaringan yang memungkinkan.

2. Hanya Kegiatan yang terdaftar atau dikenal yang dapat melewati atau melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat dipilih sekaligus berbagai jenis *policy* yang ditawarkan.
3. *Firewall* itu sendiri haruslah kebal atau relatif kuat terhadap ancaman serangan atau kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan *Operating system* yang relatif aman.

2.2.7.2. Type *Firewall*

Berikut ini adalah tipe – tipe dari sebuah sistem keamanan jaringan *Firewall*, yaitu [15]:

1. *Screened Subnet Firewall* ini menyediakan keamanan yang sangat baik dan sangat tinggi daripada tipe *Firewall* lainnya, karena membuat *Demilitarized Zone (DMZ)* diantara jaringan internal dan jaringan eksternal.
2. *Screened Host Firewall* ini terdiri dari sebuah bastion host (host yang berupa application level gateway) dan dua router packet filtering.
3. *Dual-homed Gateway Firewall* ini sedikitnya memiliki dua *IP Address* dan dua *interface* jaringan dan apabila ada ancaman serangan dari luar dan tidak dikenal maka akan diblok.
4. *Packet-filtering Firewall* ini terdiri dari router diantara jaringan internal dan eksternal yang aman. Tipe ini untuk menolak dan mengijinkan trafik.

2.2.7.3. Fungsi *Firewall*

Adapun fungsi dari sebuah *Firewall* adalah sebagai berikut [15].

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan, *Firewall* harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi *Firewall*
2. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat
3. Melakukan autentifikasi terhadap akses

4. *Firewall* mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi
5. Mencatat setiap transaksi kejadian yang terjadi di *firewall*. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan

2.2.7.4. Jenis *Firewall*

Adapun jenis – jenis sebuah sistem keamanan *firewall* adalah sebagai berikut [7].

1. *Personal Firewall*

   Firewall yang didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.

2. *Network Firewall*

   Firewall yang didesain untuk melindungi jaringan secara keseluruhan dari berbagai ancaman serangan.

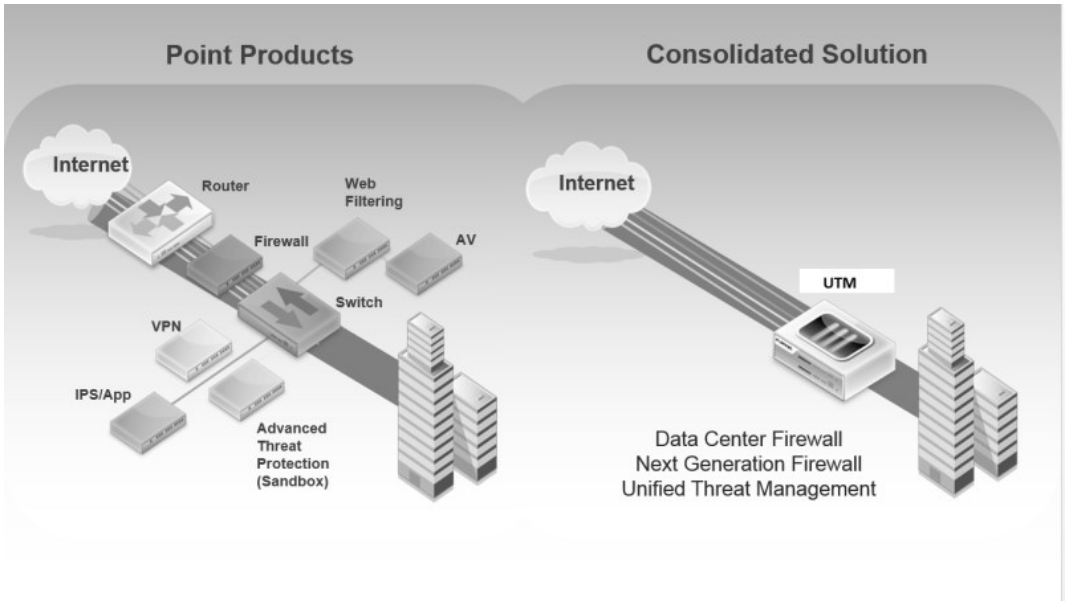
2.2.7.5. Cara Kerja *Firewall*

Berikut ini tahapan cara kerja dari sebuah sistem keamanan *Firewall* [15].

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 intenal ke *internet*. Contoh nya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
3. Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan seperti situs yang terdeteksi mengandung virus.

2.2.8. *Unified Threat Management* (UTM) *Firewall* Berbasis Linux

Unified Threat Management (UTM) Firewall berbasis Linux adalah istilah pertama kali digunakan oleh *International Data Corporation (IDC)* untuk menggambarkan kategori *device* keamanan yang mengintegrasikan berbagai fitur keamanan menjadi *single device*. *Device UTM firewall* menggabungkan kemampuan *Firewall, gateway anti-virus*, *detection intrusion* dan pencegahan ke dalam *satu platform* [8].



***Gambar 2. 13 Teknologi Unified Threat Management (UTM) Firewall* Berbasis Linux**

(*Sumber https://protokoljaringan.com/2013/12/protokol-jaringan2.jpg)*

Sistem keamanan jaringan *Unified Threat Management* (UTM) *firewall* ini memiliki keunggulan, yaitu:

1. Sebuah alat *UTM firewall* menawarkan banyak keuntungan kunci untuk mengelola ancaman data dan melindungi jaringan dan informasi sensitif. Berikut adalah beberapa keuntungan dari penggelaran alat *UTM Firewall*.
2. Konsolidasi *Hardware*: Administrator dapat membeli, menyebarkan dan mengelola salah satu alat dalam *SMB*, atau sejumlah kecil *device* di lingkungan yang lebih besar, daripada beberapa perangkat. Manajemen yang disederhanakan dan *patching*: ancaman *Blended* dan ancaman yang muncul

dapat menargetkan berbagai bagian dari jaringan secara bersamaan, menyebabkan mimpi buruk administratif jika banyak perangkat keamanan yang terlibat. *UTM firewall* menawarkan manajemen terpusat, memungkinkan administrator untuk mengelola berbagai macam ancaman terhadap lingkungan lokal dan *remote* dari konsol tunggal. *Manajemen patch* juga disederhanakan karena hanya satu atau relatif sedikit *device* perlu ditambal daripada banyak perangkat yang berbeda.

3. Satu vendor, satu lisensi, satu dukungan hubungi: Administrator dapat bekerja dengan vendor tunggal dan departemen dukungan, membina hubungan yang solid yang mempromosikan kelangsungan. Perizinan satu alat mudah untuk mengelola, bahkan sebagai kebutuhan organisasi tumbuh.
4. Beban yang lebih rendah: Konsolidasi *hardware* menawarkan titik harga yang lebih rendah dibandingkan dengan mengakuisisi beberapa perangkat, dan administrator dapat fokus pengetahuan dan pelatihan mereka pada satu alat.



Gambar 2. 14 Keunggulan Unified Threat Management (UTM) Firewall

(*Sumber https://protokoljaringan.com/2013/12/protokol-jaringan2.jpg)*

Adapun sistem operasi yang mendukung terhadap *Unified Threat Management* ini adalah sebagai berikut.

1. *Linux Zentyal*

Zentyal adalah *Server* Linux untuk *Small Business* (UMKM), yang mampu mengelola semua layanan jaringan terpadu dalam satu *platform*. *Zentyal* menyediakan *Network Gateway*, pengelola Infrastruktur, *UTM* (*Unified Threat Management*), *server* untuk perkantoran dan *Communications Server*. Semua fitur

telah terintegrasi dan mudah di-konfigurasi dengan GUI yang membantu administrator hemat waktu [9].

2. *Endian Firewall*

Endian Firewall adalah *Endian Firewall* adalah distro linux, yang berfungsi untuk *Firewall* dan *proxy.* Sangat mudah menginstall dan memiliki banyak kemampuan. *Web* Proxy dengan dukungan fitering yang lengkap. *Filtering* untuk lalu lintas *email* (*POP* dan *SMTP*) dan tentunya *open source* dengan dukungan komunitas yang luas [10].

3. *Sophos*

Sophos adalah *Unified Threat Management* membuat keamanan sederhana Sophos UTM memberikan paket keamanan jaringan utama dengan segala sesuatu yang dibutuhkan dalam alat modular tunggal. Ini menyederhanakan keamanan IT user tanpa kompleksitas solusi multi-point. Antarmuka intuitif akan membantu user dengan cepat membuat kebijakan untuk mengendalikan risiko keamanan. Dan jelas, laporan rinci akan memberikan user wawasan yang dibutuhkan untuk meningkatkan kinerja jaringan dan perlindungan [11].

2.2.9. Sistem Operasi

1. Windows

Microsoft Windows atau yang lebih dikenal dengan sebutan *Windows* adalah keluarga sistem operasi yang dikembangkan oleh *Microsoft* dengan menggunakan antarmuka pengguna grafis.

2. Linux

Linux awalnya merupakan varian dari *UNIX* untuk arsitektur *IBM.* Versi awal dituliskan oleh Linux Torvalds, seorang mahasiswa ilmu komputer dari Firlandia. Torvalds memposting versi awal Linux di *Internet* tahun 1991. Karena *Linux* gratis dan sumber kodenya tersedia, menjadi alternative awal untuk *workstation UNIX* seperti yang ditawarkan oleh *Sun Microsystem*, *Digital Equipment Corp* dan S*ilicon Graphich*. *Redhat* merupakan salah satu sistem operasi komputer turunan dari *linux* yang berfokus pada *server* dan *security* dengan dukungan *developer* yang tinggi [12].

2.2.10. Aplikasi

Berikut ini adalah aplikasi – aplikasi yang digunakan dalam analisis dan implementasi sistem keamanan jaringan menggunakan *Unified Threat Managaement* (UTM) *Firewall.*

1. *Nessus*

Nessus adalah *scanner* keamanan jaringan yang harus digunakan oleh administrator system. Nessusadalah *software* yang gratis dan bebas di download. *Nessus* merupakan sebuah *software* scanning, yang dapat digunakan untuk meng-audit keamanan sebuah sistem, seperti *vulnerability, misconfiguration, security patch* yang tidak diaplikasikan. *Default password* dan d*enial of service Nessus* berfungsi untuk monitoring lalu-lintas jaringan. Dikarenakan fungsi dari *Nessus* dapat digunakan untuk mendeteksi adanya kelemahan ataupun *bugs* tdari suatu sistem maka *Nessus* menjadi salah satu *device* andalan ketika melakukan audit keamanan suatu sistem. Dahulu sebelum *Nessus* versi 3, aplikasi ini bersifat *open source* dan menjadi salah satu primadona di dunia *open source*. Namun sekarang mulai *Nessus* versi 3 oleh *Teenable Security* dijadikansebagai aplikasi *propietary* dan *closed source* [13].

2. *VMware Workstation*

VMware Workstation adalah sebuah perangkat lunak mesin virtual untuk arsitektur komputer x86 dan x86-64 dari *VMware*, sebuah bagian dari *EMC Corporation.* Perangkat lunak ini digunakan untuk membuat banyak *x86* dan *x86-64* komputer *virtual* dan digunakan secara simultan dengan sistem operasi yang digunakan [14].

3. Wireshark

Wireshark merupakan salah satu dari *software* monitoring jaringan yang biasanya banyak digunakan oleh para administrator jaringan untuk mengcapture dan menganalisa kinerja jaringan. Salah satu alasan kenapa *Wireshark* banyak dipilih oleh seorang administrator adalah karena *interface* nya menggunakan *Graphical User Unit* (GUI) atau tampilan grafis [15].

4. OpenVPN

OpenVPN adalah aplikasi *open source* untuk *Virtual Private Networking* (VPN), dimana aplikasi tersebut dapat membuat koneksi *point-to-point tunnel* yang telah enkripsi. *OpenVPN* menggunakan *private keys*, *certificate*, atau *username* atau *password* untuk melakukan authentikasi dalam membangun koneksi [16].

2.2.11. Endian Firewall

Endian Firewall adalah perangkat lunak khusus yang berfungsi sebagai *Router, Firewall* dan Gateway berbasis Linux yang didistribusikan Oleh sebuah perusahaan yang memegang lisensi *Endian* yaitu *South Tyrolean*. *Endian Firewall* tersedia dalam bentuk, perangkat lunak komersial, perangkat keras yang dan perangkat lunak yang *open source*. *Endian Firewall* merupakan perangkat lunak pengembangan dari *FIREWALL* Versi 1.4.2 dan *Smoothwall GPL* version v0.9.9. *Endian* Memiliki komunitas untuk mengembangkan dan menutup bugs yang ada didalam *Endian Firewall* [17].

Endian Firewall adalah distro *Security* merupakan solusi Manajemen Keamanan Terpadu yang independen *Unified Threat Management* (*UTM*). Basis *Endian Firewall* adalah sistem *Operasi Linux*. *Management* dan *configuration* ijalankan melalui web base yang dapat dijalankan dari komputer lain yang terhubung melalui jaringan atau dapat melalui *Port* serial untuk mengakses sistemnya.

Tugas utama dari *Endian Firewall* adalah *GateWay, Router,* dan *Firewall,* dapat juga dijadkikan sebagai *proxy* untuk *server Web, email, FTP, SIP,* dan *DNS.*

Fitur utama termasuk stateful *Firewall* paket pemeriksaan, *proxy* level aplikasi untuk berbagai *protokol (HTTP, POP3, SMTP)* dengan dukungan antivirus, *virus* dan *spam filtering* untuk lalu lintas *email (POP* dan *SMTP),* penyaringan konten dari lalu lintas *Web* dan "kerumitan gratis" solusi *VPN* (berdasarkan *OpenVPN*).

Selain itu, distribusi menyediakan keamanan yang kuat untuk kedua jaringan lokal dan *Internet*, akan mengamankan *email user, multi-WAN* dengan

failover, routing, Network Address Translation (NAT), pelaporan dan *logging,* dipercaya *timestamping,* serta paling *UMTS modern / USB dongle 3G.* Berikut secara lengkapnya fitur yang dimiliki distro linux endian antar lain:

Tabel 2. 4 *Feature Endian Firewall*

No	Nama *Feature*
1	*Stateful Firewall*
2	*Email Security*
3	*Intrusion Prevention (IPS)*
4	*Hotspot (Captive Portal)*
5	*Quality of Service (QoS)*
6	*High Availability (Hardware Failover)*
7	*Web Security*
8	*VPN (OpenVPN dan IPSec),*
9	*Antivirus, Multi-WAN (with Failover),*
10	*Centralized Management*
11	*RePorting*
12	*Advanced Content Security*
13	*Mail and Web Security*
14	*Secure Remote Access*
15	*Live Network Monitoring* dan *RePorting*
16	*Wi-Fi* dan *Bring Your Own Device (BYOD)*
17	*Centralized Management* dan*Updates dan Application Control*

2.2.12. Pengujian *Blackbox*

Pengujian *Blackbox* berfokus pada fungsional perangkat lunak, pengujian ini dapat mendefinisikan kumpulan input dan melakukan pengetesan pada spesifikasiprogram.