BAB II
TINJAUAN PUSTAKA

Pada bab ini akan diuraikan teori–teori umum dan khusus yangberhubungan dengan penelitian tugas akhir diantaranya pengembangan sistemyang digunakan oleh penulis, teori-teori jaringan komputer, *VPN*, dan sekilastentang *Port Knocking*.

2.1 Tempat Penelitian Tugas Akhir

2.1.1 Padmanet

Merupakan suatu unit usaha yang bergerak di bidang Informasi dan Teknologi, fungsi utama dari padmanet yaitu memberikan palayanan jasa koneksi internet, intergrasi antar unit dalam bentuk WAN (Wide Area Network), pusat data dan informasi internal, serta pelayanan service kepada masyarakat luas dalam penyediaan teknologi informasi

2.1.2 Dokumen Imigrasi

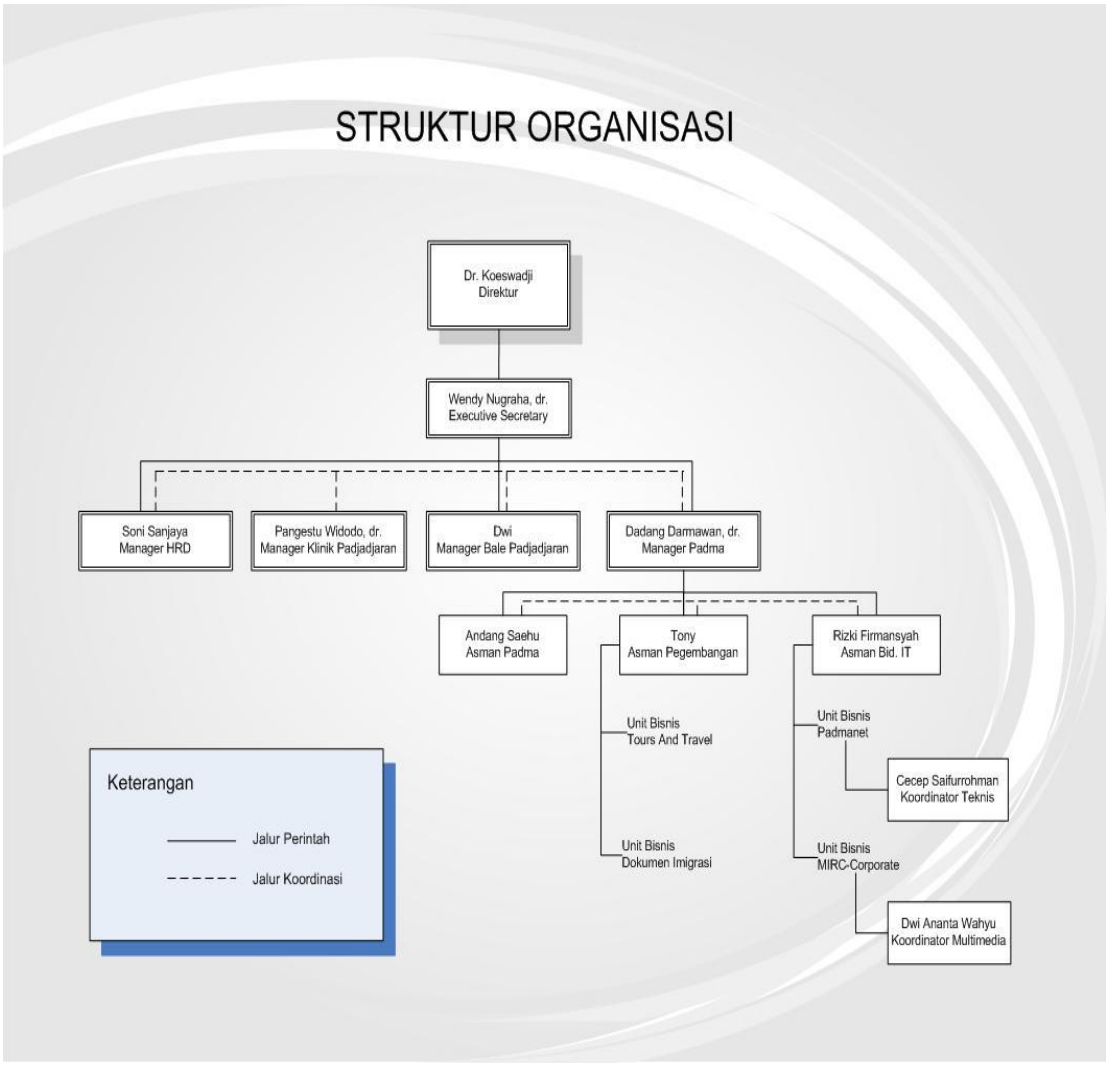
Merupakan unit pelayanan dokumen keimigrasian untuk mahasiswa asing yang belajar di Indonesia dan pelayanan dokumen imigrasi untuk masyarakat luas pada umumnya.

2.1.3 Tours and Travel

Merupakan unit usaha dalam penyediaan keperluan hiburan dan perjalanan wisata lainnya, termasuk juga dalam penyediaan tiket transportasi (darat dan udara) serta pelananan dalam penyediaan hotel.

2.1.4 MIR-C Corporate

Memiliki sumberdaya manusia dengan latar belakang pengalaman bekerja di lingkungan pendidikan kedokteran dan kesehatan, serta tenaga pelaksana yang profesional mulai dari desain, produksi sampai pasca produksi maka dihasilkan produk-produk bernuansa kedokteran yang berkualitas.



Gambar 2. 1 Struktur Organisasi

2.1.5 Padjadjaran Mitra Net

PadmaNet adalah bidang usaha yang di bangun sebagai penyedia jasa solusi di bidang Teknologi Informasi bagi anda. Melalui keberadaan kami, kami berusaha memajukan pengetahuan masyarakat akan teknologi informasi dan juga memenuhi kebutuhan yang diiringi oleh permintaan akan hal ini. Sebagai bidang usaha yang memposisikan diri sebagai konsultan, kami menawarkan jasa kami untuk berbagai aspek kebutuhan yang anda butuhkan.

1. Pembangunan Perangkat Lunak

Sistem terkomputerisasi tidak dapat dipungkiri menawarkan kecepatan dan akurasi data. Bagi anda atau instansi yang membutuhkan aplikasi untuk proses bisnis, kami menawarkan jasa analisis proses dan pembuatan program yang sesuai dengan kebutuhan anda.

2. Instalasi Jaringan Komputer

Konsep networking telah terbukti mampu menekan angka investasi suatu proses bisnis. PadmaNet hadir bagi anda yang membutuhkan tenaga ahli untuk menciptakan suatu sistem komputer yang terhubung dalam jaringan (intranet / internet).

Selain menawarkan jasa, melalui sistem support, kami juga berusaha menyediakan media komunikasi dua-arah, yang memfasilitasi antara anda dan kami. Tulisan-tulisan yang ada disini adalah disajikan sebagai informasi bagi anda yang membutuhkan. Karena kami berpikir bahwa peluang yang kami peroleh, sudah sepatutnya dibagikan kepada siapa saja. Dan bukanlah sesuatu yang ekslusif untuk dikonsumsi oleh kalangan tertentu saja.

2.2. Visi Dan Misi Padjadjaran Mitra Net

2.2.1. Visi

Menjadi unit bisnis jasa teknologi informasi terdepan yang terpercaya.

2.2.2. Misi

Menyebarkan dan memberdayakan kemajuan teknologi informasi khususnya dalam kalangan pendidikan dan umumnya kepada masyarakat luas, dengan menciptakan infrastruktur yang kuat dan handal, menyediaan layanan

teknologi informasi, dengan pengembangan usaha yang tinggi dan memberikan manfaat dan profitabilitas yang optimal.

Goals Dengan Tujuan membangun Teknologi Informasi Indonesia, PadmaNet memberikan banyak fasilitas dan inovasi untuk memecahkan permasalahan dalam Teknologi Informasi. Fasilitas yang diberikan secara keseluruhan menjadikan PadmaNet sebagai software house dan local provider yang dapat menjadi portal kelancaran usaha anda dengan cara membangun relasi yang baik antara komunitas, client dan PadmaNet.

Produk PadmaNet diantaranya

1. Internet Access

   Akses internet global memungkinkan anda untuk mengaskes internet 24 jam browsing web, email, chat, e-commerce, hotnews dll.

2. IIX Acess

   Akses internet khusus koneksi lokal (Indonesia) solusi paling efisien untuk sharing data dan komunikasi data secara local.

3. Infrastruktur Networking / Jaringan

   Pembangunan infrastruktur network / jaringan bagi perusahaan untuk komunikasi data dengan menggunakan teknologi wireless maupun kabel, dengan installasi server berbasis linux, unix dan freeBSD. Anda juga akan mendapat service berupa maintenace jaringan bila diperlukan. Kami siap untuk membangun jaringan komputer anda dengan teknologi wireless 2.4 Ghz dengan daya jangkau luas yang sangat bermanfaat bagi anda yang ingin menghubungkan kantor - kantor anda dalam satu jaringan komputer terpadu.

4. VPN Akses

   Akses internet dengan kabel atau menggunakan perangkat radio wireless, anda cukup menggunakan wifi atau kabel dan laptop anda akan terhubung ke internet dengan melakukan tunneling *PPTP* terhadap server vpn ,anda cukup mengisi username dan password untuk Authentication dan anda terhubung ke internet.

5. Application software

   Kebutuhan akan aplikasi komputer penunjang pekerjaan semakin meningkat, untuk itu kami berusaha memenuhi kebutuhan anda dengan

memberikan layanan dibidang software programing. Software yang kami desain bukanlah sekedar software yang bisa berfungsi saja, tetapi kami memberikan solusi melebihi yang anda minta. Setiap software yang kami hasilkan akan terlebih dahulu kami uji stabilitas, keamanan dan perfomancenya.

2.3. Pengguna Jasa Padjadjaran Mitra Net

Adapun yang menjadi pengguna jasa adalah seluruh perusahaan ataupun individu dari seluruh layanan produk. Beberapa perusahaan yang telah menggunakan jasa PadmaNet, antara lain:

2.3.1. Klinik Padjadjaran (Divisi Kesehatan PT RSP)

1. Sistim Informasi Klinik (SIKI)
    1. SIKI V.1, V.2, V.3
    2. SIKI CNP (Clinik Network Program)
    3. SIKI Versi Single Dokter

2. Pembangunan Infrastruktur Networking
    1. Fix Line
    2. Hotspot system
3. Pembangunan Server aplikasi (Linux based)
4. Pembuatan Office Online

2.3.2. Fakultas Kedokteran Unpad

1. Pembuatan Website Asian Education Conference (Amea 2009)

Homepage: http://amea2009.fk.unpad.ac.id

2. Penyediaan Layanan Internet

2.3.3. Fakultas Kedokteran Unisba

Pemeliharaan Infrastruktur IT dan konsultan IT Unisba

2.3.4. Bale Market

Pembuatan Sistim Informasi Mini Market

2.3.5. Organisasi Penanggulangan dan penyuluhan HIV/AIDS IMPACT

Pembuatan website impactHomepage :http://www.impactbandung.org

2.4 Teknologi Jaringan Komputer

Definisi jaringan komputer adalah terhubungnya dua komputeratau lebih dengan kabel penghubung (pada beberapa kasus, tanpa kabel atau wireless sebagai penghubung),sehingga antar komputer dapat saling tukar informasi(data) [**1**].

Tujuan dari jaringan komputer adalah:

1. Membagi sumber daya : contohnya berbagi pemakaian printer, CPU,memori, harddisk dan lain-lain.
2. Komunikasi : contohnya e-mail, instant messaging, chatting.
3. Akses informasi :contohnya web browsing, file server dan lain-lain

Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringankomputer meminta dan memberikan layanan. Pihak yang meminta layanandisebut klien (client) dan yang memberikan layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem client-server, dan digunakanpada hampir seluruh aplikasi jaringan komputer [**1**].

2.4.1 OSI Layer (Open System Interconnect)

Sebuah arsitektur model komunikasi data (disebut Open SystemInterconnect atau OSI Refference Model) telah dibuat oleh International Standards Organization (ISO) yang ditujukan untuk menemukan strukturdan fungsi protokol komunikasi data pada berbagai tingkat komunikasi di dalam jaringan komputer [**1**].

Model OSI berisi tujuh lapis (layer) yang menentukan fungsi protokol komunikasi data. Setiap lapis yang ada dalam model OSI memiliki fungsi dalam komunikasi data didalam jaringan computer [**1**].

a) Physical Layer

Physical layer yaitu lapisan fisik yang berkaitan dengan elektronik dari komputer ke Local Area Network melalui Ethernet Card atau perangkat

wireless atau perangkat modem satelit atau perangkat modem leased line. Perangkat elektronik yang digunakan ini memberikan karakteristik fisik media jaringan komputer [**1**].

b) Data link Layer

Data link layer yaitu lapisan data berisi ketentuan yang mendukung sambungan fisik seperti penentuan biner 0 dan 1, penentuan kecepatan penentuan biner terebut dan lainnya agar sambungan jaringan komputer bisa berjalan baik. Dengan kata lain Data link layer menterjemahkan sambungan fisik menjadi sambungan data.

c) Network Layer

Network layer yaitu memungkinkan perangkat yang tersambung menyebutkan perbedaan yang ada antara satu komputer dengan komputer lainnya. Aliran pengalamatan dan komunikasi dasar ini ditangani oleh network layer. Lapisan ini juga menentukan kaidah jumlah informasi yang dapat di kirim di dalam sebuah paket data dan koreksi erornya [**1**].

d) Transport Layer

Paket data yang mengalir dari host ke host bisa datang atau tidak datang ketika paket itu dikirimkan. Dengan berbagai alasan seperti karena adanya kesalahan rute (error routing) dan kesalahan network (error network), paket data yang dikirimkan dari sebuah host ke host lain bisa saja tidak sampai ke tujuan. Lapisan transport ini menyusun ulang perintah pengiriman paket data ke dalam urutan yang benar dan biasanya memakai mekanisme pengecekan untuk menemukan apakah paket telah tiba di tujuan atau belum. Transport layer dapat bertanya kepada host tujuan untuk memastikan apakah paket data telah diterima atau belum. Bila belum diterima, maka akan dikirim paket data kembali. Pada layer ini protokol yang bekerjaadalah TCP (Transmission Control Protocol), UDP (User Datagram Protocol) dan SPX (Sequenced Packet Exchange) [**1**].

e) Session Layer

Session layer adalah tempat berikutnya yang akan dilalui olehpaket data yang telah diterima. Lapisan ini memakai paket data untuk menghasilkan multi sambungan [**1**].

f) Presentation Layer

Presentation layer yaitu lapisan presentasi yang berperan menyusun kembali paket data yang dikirim. Paket data yang dikirim selalu berupa pecahan paket data. Ada kira kira 10 buah pecahan paket data yang dibuat dari sebuah data. Pecahan ini setelah diterima dengan baik, oleh lapisan presentasi akan disusun ulang sesuai dengan data aslinya. Aplikasi yang bekerja pada layer presentasi adalah; PICT, TIFF, JPEG, merupakan format data untuk aplikasi bergambar, lalu aplikasi MIDI dan MPEG untuk aplikasi sound dan movie. Pada aplikasi web, HTTP [**1**].

g) Application Layer

Application layer adalah tempat dimana program dapat memesan, meminta servis yang terdapat di dalam sebuah jaringan komputer seperti file transfer, otentikasi pengguna atau melacak database. Dalam hal Internet, protokol seperti ini adalah FTP, Telnet, Gopher, World Wide Web, dan lain lain [**1**].

Tabel 2. 1 Standar pada OSI Layer

ISO pada Model OSI Layer		
Layer	**Fungsi**	**Protocol atauStandar**
Layer 7: Application	Menyediakanlayanan e-mail, transfer file dan file server.	FTP, TFTP, DNS, SMTP, SFTP, SNMP,Rlogin, BootP, MIME
Layer 6: Presentation	Menyediakanenskripsi, konversikode, danmemformat data.	JPEG, HTTP, MPEG, TIFF
Layer 5: Session	Menegosasihubungandengankomputer lain.	SQL, X-Window, ASP, NFS
Layer 4: Transport	Mendukungpenerimaan data pada end-to-end daripengirim.	TCP, UDP, SPX
Layer 3: Network	Menampilkanpaket routing padajaringanseberang.	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2: Data link	Menyediakancek error dan transfer pada frame pesan.	SLIP, PPP, MTU
Layer 1: Physical	Hubungan / sambungandengan media transmisidanmengirim data padajaringan.	IEEE 802, EIA RS-232

2.4.2 Jenis-Jenis Jaringan Komputer

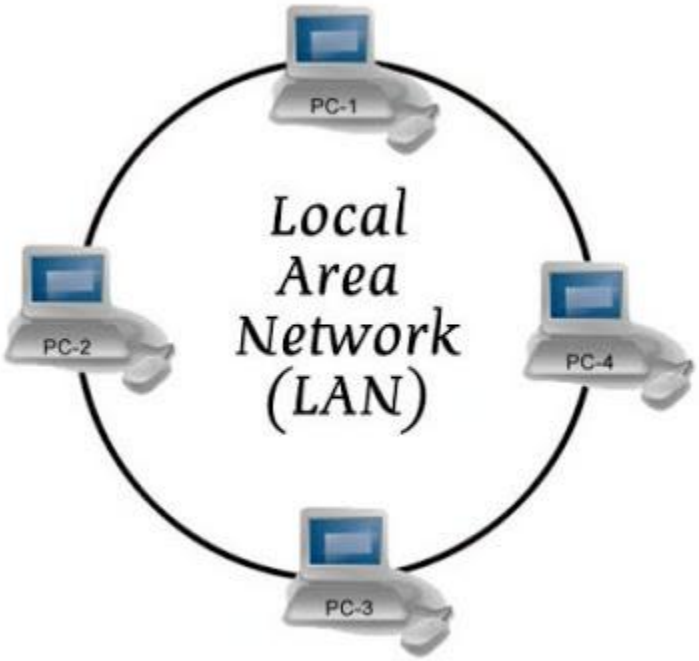
Jenis-jenis jaringan terbagi dalam dua lingkup, lingkup pertama berdasarkan geografis dan yang kedua berdasarkan service [**1**].

2.4.2.1 Berdasarkan Ruang Lingkup Geografis

Berdasarkan ruang lingkup geografis jaringan terdapat tigajenis jaringan computer [**1**].

1. Local Area Network (LAN)

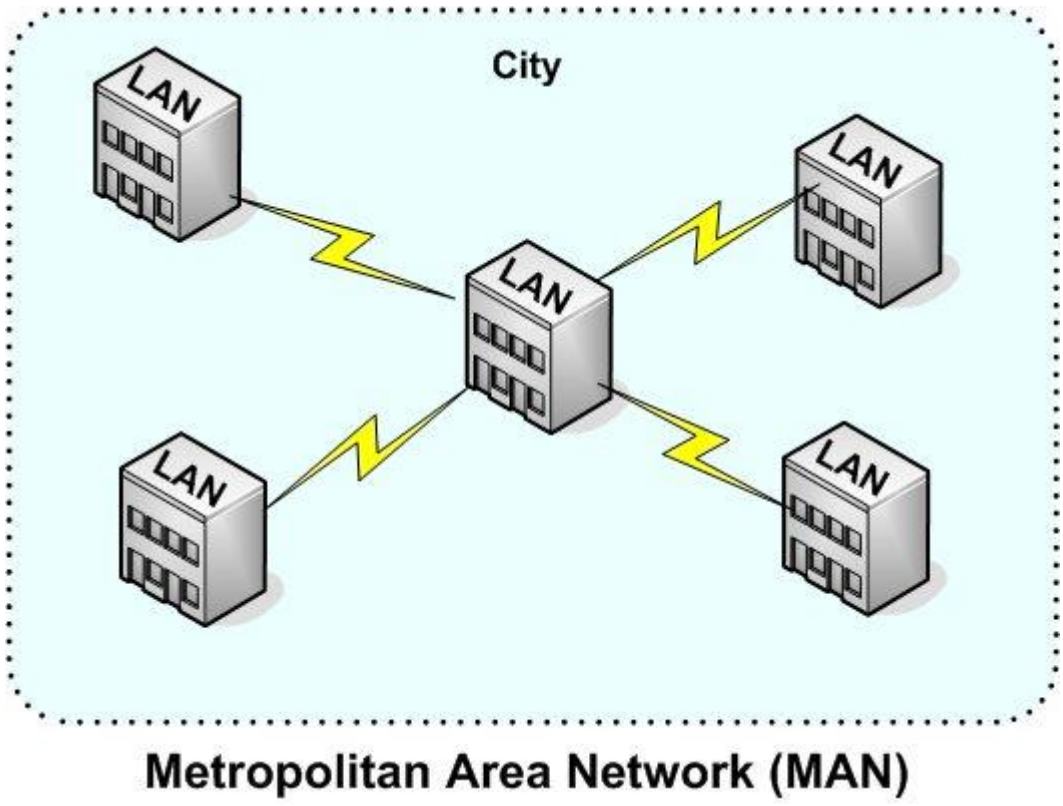
Local Area Network (LAN) adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.Beberapa model konfigurasi LAN, satu komputer biasanya di jadikan sebuah file server. Yang mana digunakan untuk menyimpan perangkat lunak (software) yang mengatur aktifitas jaringan, ataupun sebagai perangkat lunak yang dapat digunakan oleh komputerkomputer yang terhubung ke dalam network.Komputer-komputer yang terhubung ke dalam jaringan (network) itu biasanya disebut dengan workstation. Biasanya kemampuan workstation lebih di bawah dari file server dan mempunyai aplikasi lain di dalam harddisknya selain aplikasi untuk jaringan. Kebanyakan LAN menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya [**1**].



Gambar 2. 2 Skema jaringan LAN

2. Metropolitan Area Network (MAN)

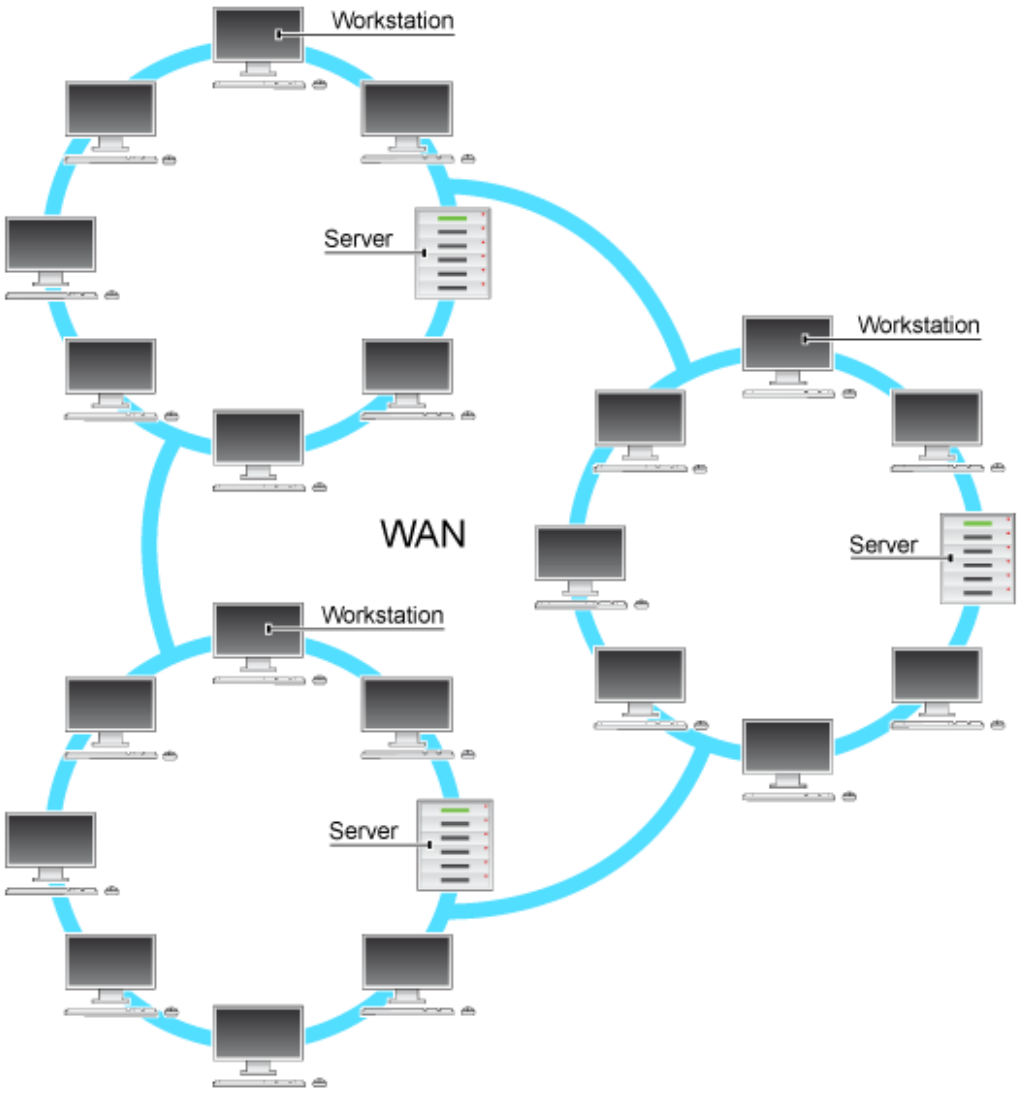
Metropolitan Area Network (MAN) biasanya meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu propinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan Kantor pusat pada suatu bank dimana beberapa kantor cabang sebuah bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya. Misalnya bank tersebut yang ada di seluruh wilayah Jakarta [**1**].



Gambar 2. 3 Skema Jaringan MAN

3. Wide Area Network (WAN)

Wide Area Network (WAN), adalah kumpulan dari Local Area Network (LAN) dan/atau Workgroup yang dihubungkan dengan menggunakan alat komunikasi, umumnya menggunakan modem untuk membentuk hubungan dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan cepat serta dengan biaya relatif murah [**1**].



Gambar 2. 4 Skema Jaringan WAN

2.4.2.2 Berdasarkan Service

Berdasarkan service jenis jaringan komputer terdapat dua jenis jaringan komputer [**2**].

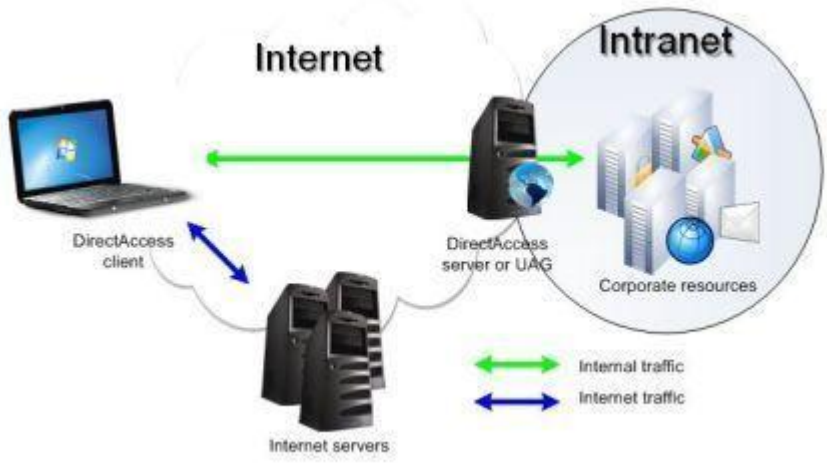
2.4.2.2.1 Internet

Internet adalah jaringan global yang memungkinkan duakomputer atau lebih berkoneksi dengannya untuk mentransfer filedan tukar-menukar email dan pesan-pesan real-time. Internet merupakan landasan untuk world wide web. Internet juga merupakan kumpulan jaringan komputer yang berbeda-beda dansaling berhubungan di seluruh dunia. Semua komputer itu dihubungkan

Internet agar dapat berkomunikasi satu sama lain dengan menggunakan TCP/IP [**2**].

2.4.2.2.2 Intranet

Intranet adalah jaringan swasta yang berdasarkan standar teknologi internet (IP) yang sejenis world wide web internal dalam suatu organisasi. Intranet adalah penggunaan teknologi internet dalam pada jaringan internal suatu perusahaan berdasarkanteknologi web. Intranet hanya eksis di dalam organisasi, sedangkan internet adalah jaringan global yang terbuka bagi semua orang.Intranet berhubungan erat dengan internet. Internet dan intranet berbagi perangkat lunak dan peralatan jaringan yang sama, dan berbicara dengan bahasa yang sama pula. Intranet dijalankan pada internal perusahaan dan pada antar kantor cabang perusahaan mereka, serta tertutup bagi internet dari luar dengan menggunakan firewall yang memungkinkan para karyawan browsing ke luar, tetapi mencegah orang luar browsing ke dalam [**2**].



Gambar 2. 5 Jaringan Intranet dan Internet

2.4.3 Performance

Kinerja merupakan definisikan performance selain berfungsi dengan optimal, juga kebutuhan untuk kinerja harus maksimal [**2**].

Kinerja adalah kemampuan jaringan komputer dalam menjalankan performa fungsinya. Aplikasi atau user membutuhkan kemampuan dalam jaringan komputer yang berbeda. Misalkan transfer data dalam batasan waktu tertentu online service, jumlah koneksi serentak concurrent, dan lain sebagainya, salah satu kebutuhan jaringan yaitu kinerja kecepatan yang tinggi [**2**].

Faktor yang dapat mempengaruhi kinerja :

1. Performa send receive. Faktor yang mempengaruhi pengiriman dan pernerimaan data adalah starting point ketika mengirim bits antar dua komputer direct, informasi dikirim dalam bentuk blok message packet, traffic dua arah full duplex dan internal komputer misalnya device driver mengirimkan bits write atau menerima bits read, tarsfer bits dari Network Internet Card (NIC) ke memory.
2. Bandwidth dan Latency

   Latencey, lama waktu yang diperlukan untuk megirimkan message dari ujung end ke ujung lainnya end to end. Bandwidith, jumlah bits yang dapat di-transfer dalam satu periode waktu.

2.4.4 Bandwidth dan Transfer Rate

Bandwidth adalah jumlah bits yang dapat di-transfer dalam satu periode waktu dan suatu ukuran dari banyaknya informasi yang mengalir dari suatu tempat ke tempat lain dalam suatu waktu tertentu. Bandwidth dapat dipakaikan untuk mengukur baik aliran data analog maupun aliran data digital. Sekarang telah menjadi umum jika kata bandwidth lebih banyak dipakaikan untuk mengukur aliran digital [**2**].

Bandwidth tegantung kemampuan perangkat jaringan. Misalkan 1Mbits atau detik = 1 Mbps, artinya dapat mengirimkan data 1juta bit setiap detik. Bandwidth 1 Mbps memerlukan 1mikro detik untuk mengirimkan 1 detik.

Transfer rate adalah waktu rata-rata transfer paket data dari sumber sampai ke tujuan akhir.

Rumus transfer rate : *Size(byte)/Time(second)* ……..

Perbedaan bandwidth dan transfer rate, bandwidth memiliki nilaiyang statis, sedangkan transfer rate tergantung dari size dan waktu yang ditempuh sifatnya tidak statis.

2.5 Pengenalan Sistem Operasi

Istilah sistem operasi sering ditujukan kepada semua software yang masuk dalam satu paket dengan sistem komputer sebelum aplikasi-aplikasi software terinstall. Dalam Ilmu komputer, sistem operasi atau dalam bahasa Inggris: *operating system* atau OS adalah perangkat lunak sistem yang bertugas untuk melakukan kontrol dan manajemen perangkat keras serta operasi-operasi dasar sistem, termasuk menjalankan software aplikasi seperti program-program pengolah kata dan browser web. Secara umum, sistem operasi adalah *software* pada lapisan pertama yang ditaruh pada memori komputer pada saat komputer dinyalakan. Sedangkan *software-software* lainnya dijalankan setelah sistem operasi berjalan, dan sistem operasi akan melakukan layanan inti umum untuk *software-software* itu. Layanan inti umum tersebut seperti akses ke disk, manajemen memori, scheduling task, dan antar-muka user. Sehingga masing-masing software tidak perlu lagi melakukan tugas-tugas inti umum tersebut, karena dapat dilayani dan dilakukan oleh sistem operasi [**3**].

2.5.1 Sejarah Linux

Linux pada awalnya dibuat oleh seorang mahasiswa Finlandia yang *bernama Linus Benedict Torvalds*. Dulunya Linux merupakan proyek hobi yang diinspirasikan dari Minix, yaitu sistem UNIX kecil yang dikembangkan oleh Andrew Tanenbaum. Linux *versi* 0.01 dikerjakan sekitar bulan Agustus 1991. Kemudian pada tanggal 5 Oktober 1991, Linus mengumumkan versi resmi Linux, yaitu *versi* 0.02 yang hanya dapat menjalankan *shell bash(GNU Bourne Again Shell*) dan gcc (*GNU C Compile*r) [**3**].

2.5.1.1 Distribusi Linux

Terdapat banyak distribusi Linux (lebih dikenali sebagai distro) yang dibuat oleh individu, grup, atau lembaga lain. Masing-masing disertakan dengan

program sistem dan program aplikasi tambahan, di samping menyertakan suatu program yang memasang keseluruhan sistem di komputer (installer program). Inti di setiap distribusi Linux adalah kernel, koleksi program dari proyek GNU (atau proyek lain), cangkang (shell), dan aturcara utilitas seperti pustaka (libraries), kompilator, dan penyunting (editor). Kebanyakan sistem juga menyertakan aturcara dan utilitas yang bukan-GNU. Bagaimanapun, utilitas tersebut dapat dipisahkan dan sistem ala UNIX masih tersedia. Beberapa contoh adalah aturcara dan utiliti dari BSD dan sistem grafik-X (X-Window System). X menyediakan antarmuka grafis (GUI) yang umum untuk Linux. Contoh-contoh distribusi Linux : Ubuntu, SuSE, Fedora, Mandriva, Slackware, Debian, PCLinuxOS, Knoppix, Xandros [**3**].

2.5.2 Sejarah Windows

Microsoft Windows atau lebih dikenal dengan sebutan Windows adalah keluarga sistem operasi komputer pribadi yang dikembangkan oleh Microsoft yang menggunakan antarmuka dengan pengguna berbasis grafik (graphical user interface) [**3**].

Dimulai dari DosShell for DOS 6 buatan Microsoft dan inginnya Microsoft bersaing terhadap larisnya penjualan Apple Macintosh yang menggunakan GUI, Microsoft menciptakan Windows 1.0. Nama ini berasal dari kelatahan karyawan Microsoft yang menyebut nama aplikasi tersebut sebagai program windows (Jendela Program). Windows versi 2 adalah versi Windows pertama yang bisa diinstal program. Satu-satunya program yang bisa ditambahkan adalah Microsoft Word versi 1. Windows versi 3 menjanjikan aplikasi tambahan yang lebih banyak, kelengkapan penggunaan, kecantikan user interface atau antarmuka dan mudahnya konfigurasi [**3**].

Windows versi 3.1 adalah versi Windows yang bisa mengoptimalisasi penggunaannya pada prosesor 32-bit Intel 80386 ke atas. Windows versi 3.11 adalah versi Windows terakhir sebelum era *Start Menu*. Windows 3.11 pun adalah *versi* Windows pertama yang mendukung *networking*/jaringan. *Versi Hibrida* dapat dijalankan tanpa MS-DOS. *Versi Hibrida* tersebut menginstalasi dirinya

sendiri dengan DOS 7. Tidak seperti Windows versi 16-bit yang merupakan shell yang harus diinstalasi melalui DOS terlebih dahulu. Aplikasinya pun berbeda. Meskipun Windows 9X dapat menjalankan aplikasi Windows16-bit, namun Windows 9X memiliki grade aplikasi sendiri -X86-32, Windows 9X sangat terkenal dengan BSOD (Blue Screen of Death) [**3**].

2.5.2.1 Versi-versi Windows

Versi dari Windows sudah banyak yang telah diliris dari tahun 1985 sampai dengan tahun 2008, seperti ditunjukkan tabel 2.2 dibawah ini [**3**].

16-bit, berjalan di atas MS-DOS

- 1985 November - Windows 1.0
- 1987 9 Desember - Windows 2.0
- 1990 22 Mei - Windows 3.0
- 1992 Agustus - Windows 3.1
- 1992 Oktober - Windows for *Workgroups* 3.1
- 1993 November - Windows for *Workgroups* 3.11

Hibrida (16-bit/32-bit), berjalan tanpa MS-DOS (meski tidak sepenuhnya)

- 1995 24 Agustus - Windows 95 (Versi: 4.00.950)
- 1998 25 Juni - Windows 98 (Versi: 4.1.1998)
- 1999 5 Mei - Windows 98 Second Edition (Versi: 4.1.2222)
- 2000 19 Juni - Windows *Millennium Edition* (Me) (Versi: 4.9.3000)

Berbasis kernel Windows NT

- 1993 Agustus - Windows NT 3.1
- 1994 September - Windows NT 3.5
- 1995 Juni - Windows NT 3.51
- 1996 29 Juli - Windows NT 4.0
- 2000 17 Februari - Windows 2000 (Versi: NT 5.0.2195)
- 2001 - Windows XP (Versi: NT 5.1.2600)
- 2003 - Windows Server 2003 (Versi: NT 5.2.3790)
- 2006 - Windows Vista (Versi 6.0 Build 6000)
- 2007 - Windows Home Server (Versi 6.0.1800.24)

- 2008 - Windows Server 2008 (Versi 6.1)
- 2009 - Windows 7 (Versi 6.1 Build 7600)
- 2009 - Windows Server 2008 R2 (Versi 6.1)
- 2011 - 2012 - Windows 8.1

2.6 Kompresi Dekompresi

Kompresi adalah proses pengubahan sekumpulan data menjadi satu bentuk kode untuk menghemat kebutuhan tempat penyimpanan dan waktu untuk transmisi data. Ada beberapa faktor yang sering menjadi pertimbangan dalam memilih suatu metode kompresi yang tepat, yaitu kecepatan kompresi, sumber daya yang dibutuhkan memory, kecepatan PC, ukuran file hasil kompresi, besarnya redundansi dan kompleksitas algoritma. Tidak ada metode kompresi yang efektif untuk semua jenis file.

Pengiriman data hasil kompresi dapat dilakukan jika pihak pengirim yang melakukan kompresi dan pihak penerima melakukan aturanyang sama dalam hal kompresi data. Pihak pengirim harus menggunakan algoritma kompresi yang sudah baku dan pihak penerima juga menggunakan teknik dekompresi data yang sama dengan pengirim sehingga data yang diterima dapat dibaca atau di-decode kembali dengan benar.

Kompresi data menjadi sangat penting karena memperkecil kebutuhan penyimpanan data, mempercepat pengiriman data, memperkecil kebutuhan bandwidth. Teknik kompresi dilakukan terhadap data text biner atau gambar [**4**].

2.7 Enkripsi Dekripsi

Encryption atau enkripsi merupakan proses untuk mengubah sebuah pesan informasi sehingga tidak dapat dilihat tanpa menggunakan kunci pembuka. Enkripsi adalah cara yang paling efektif untuk memperoleh pengamanan data. Untuk membaca file yang dienkrip, kita harus mempunyai akses terhadap kata sandi yang memungkinkan kita mendekrip pesan tersebut. Data yang tidak dienkrip disebut plaintext, sedangkan yang dienkrip disebut ciphertext.

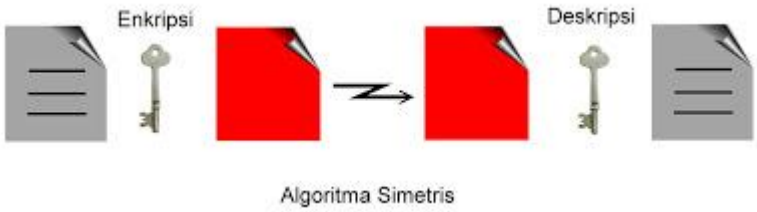
Sebuah pesan dalam bentuk plaintext diubah dengan encryption menjadi ciphertext. Proses sebaliknya, untuk mengembalikan ciphertext ke-plaintext disebut decryption atau dekripsi.

Teknologi enkripsi bukan hanya milik VPN saja, namun sangat luas pengunaannya. Enkripsi bertugas untuk menjaga privasi dan kerahasiaan data agar tidak dapat dengan mudah dibaca oleh pihak yang tidak berhak. Secara garis besar teknik enkripsi terbagi atas dua jenis symmetric encryption dan asymetric encryption [**4**].

2.7.1 Enkripsi Simetris

Enkripsi Simetris dikenal juga dengan nama sebutan secret key encryption. Enkripsi jenis ini banyak digunakan dalam proses enkripsi data dalam volum yang besar. Selama masa komunikasi data, perangkat jaringan yang memiliki kemampuan enkripsi jenis ini akan mengubah data yang berupa teks murni (cleartext) menjadi berbentuk teks yang telah diacak atau istilahnya adalah ciphertext. Teks acak ini tentu dibuat dengan menggunakan algoritma. Teks acak ini sangat tidak mudah untuk dibaca, sehingga keamanan data terjaga.

Pertanyaan selanjutnya, bagaimana data acak tersebut dibuka oleh pihak yang memang ditujunya. Untuk membuka data acak ini, algoritma pengacak tadi juga membuat sebuah kunci yang dapat membuka semua isi aslinya. Kunci ini dimiliki oleh si pengirim maupun si penerima data. Kunci inilah yang digunakan dalam enkripsi dan dekripsi ciphertext ini [**4**].



Gambar 2. 6 Enkripsi Simetris

Digital Encryption Standar (DES) merupakan sebuah algoritma standar yang digunakan untuk membuat proses symmetric encryption ini. Algoritma ini diklaim sebagai yang paling umum digunakan saat ini. Algoritma DES beroperasi dalam satuan 64-bit blok data. Maksudnya, algoritma ini akan menjalankan serangkaian proses pengacakan 64-bit data yang masuk untuk kemudian dikeluarkan menjadi 64-bit data acak. Proses tersebut menggunakan 64-bit kunci

di mana 56-bitnya dipilih secara acak, 8 bit nya berasal dari parity bit dari data. Kedelapan bit tersebut diselipkan di antara ke 56-bit tadi. Kunci yang dihasilkan kemudian dikirimkan ke si penerima data [**4**].

Dengan sistem enkripsi demikian, DES tidaklah mudah untuk ditaklukkan Namun seiring perkembangan teknologi, DES sudah bisa dibongkar dengan menggunakan superkomputer dalam waktu beberapa hari saja. Alternatif untuk DES adalah triple DES (3DES) yang melakukan proses dalam DES sebanyak tiga kali. Jadi kunci yang dihasilkan dan dibutuhkan untuk membuka enkripsi adalah sebanyak tiga buah.

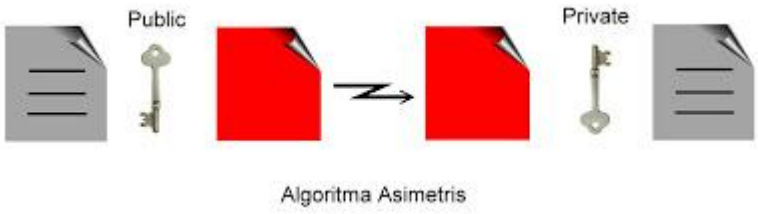
2.7.2 Enkripsi Asimetris

Enkripsi Asimetris sering disebut sebagai sistem public key encryption. Proses enkripsi jenis ini bisa menggunakan algoritma apa saja, namun hasil enkripsi dari algoritma ini akan berfungsi sebagai pelengkap dalam mengacakan dan penyusunan data. Dalam enkripsi jenis ini diperlukan dua buah kunci pengaman yang berbeda, namun saling berkaitan dalam proses algoritmanya. Kedua kunci pengaman ini sering disebut dengan istilah Public Key dan Private Key [**4**].

Mekanisme pembuatan public dan private key ini cukup kompleks. Biasanya kunci-kunci ini di-generate menggunakan generator yang menjalankan algoritma RSA (Ron Rivest, Adi Shamir, Leonard Adleman) atau EL Gamal. Hasil dari generator ini biasanya adalah dua buah susunan angka acak yang sangat besar. Satu angka acak berfungsi sebagai public key dan satu lagi untuk private key. Angka-angka acak ini memang harus dibuat sebanyak dan seacak mungkin untuk memperkuat keunikan dari kunci-kunci [**4**].

Menggenerasi kunci-kunci ini sangat membutuhkan proses CPU yang tinggi. Maka itu, proses ini tidak bisa dilakukan setiap kali melakukan transaksi data. Dengan kata lain, enkripsi jenis ini tidak pernah digunakan untuk mengamankan data yang sesungguhnya karena sifatnya yang kompleks ini. Meskipun demikian, enkripsi ini akan sangat efektif dalam proses otentikasi data

dan aplikasinya yang melibatkan sistem digital signature dan key management [**4**].



Gambar 2. 7 Enkripsi Asimetris

2.8 Teknologi Keamanan Jaringan Komputer

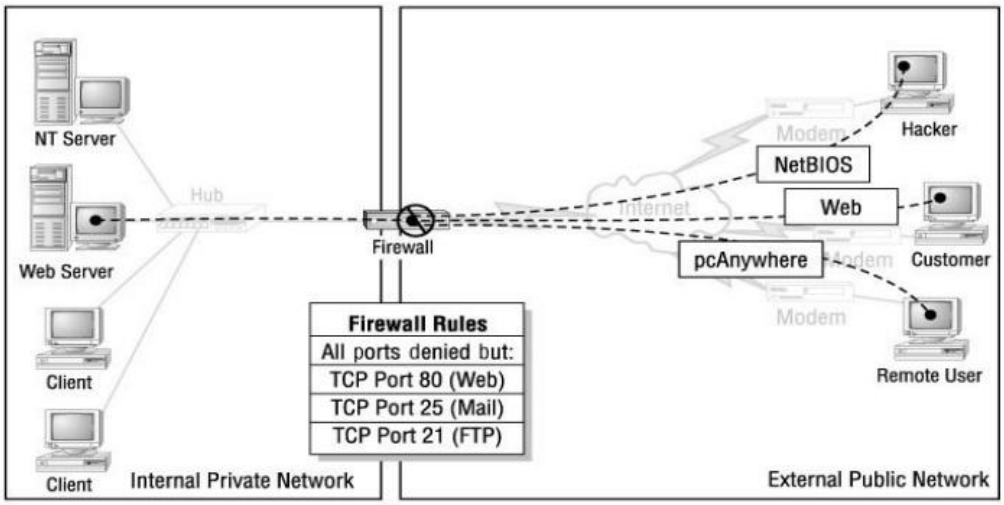
Pada teknologi keamanan jaringan komputer adalah suatu aplikasi atau sistem yang dapat mengamankan jaringan komputer pada suatu hal yang dapat menyerangnya. Sehingga contoh berikut adalah teknik pada suatu sistem keamanan jaringan komputer. Penyusun hal membatasi sistem tersebut yang menyangkut pada jaringan publik (Internet) [**5**].

2.8.1 Firewall

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Firewall adalah sebuah perangkat lunak (Software) atau perangkat keras (Hardware) yang menyaring seluruh lalu-lintas data (traffic) antara komputer kita, jaringan komputer di rumah atau di kantor dengan Internet. Firewall dalam sebuah jaringan, akan memastikan apabila terjadi hal-hal buruk yang tidak diinginkan terjadi di satu sisi firewall (misalnya sisi Internet) maka komputer yang ada di sisi lainya tidak akan terpengaruh. Fungsi dasar dari suatu firewall adalah [**5**]:

1. Packet Filtering : Seluruh header dari paket data yang melewati firewall akan diperiksa, disini firewall membuat keputusan yang jelas/tegas untuk mengijinkan atau memblok setiap paket.
2. Aplication Proxy: Firewall mampu memeriksa lebih dari sekedar header suatu paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifik.

3. Pemantauan dan pencatatan traffic: Mencatat apa-apa saja yang terjadi di firewall amatlah penting, sehingga bisa membantu kita untuk memperkirakan kemungkinan penjebolan keamanan atau memberikan umpan balik yang berguna tentang kinerja firewall.

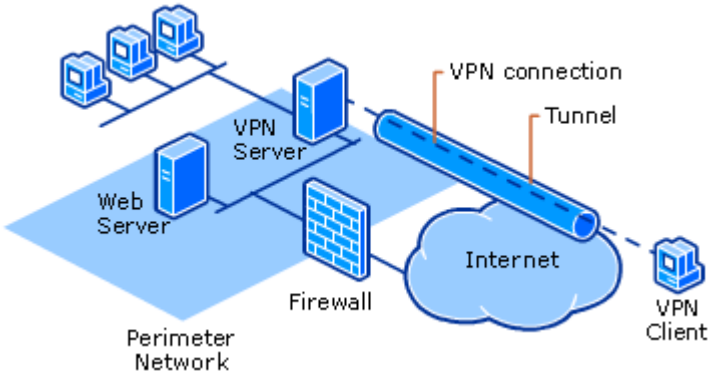


Gambar 2. 8 Firewall

2.8.2 Virtual Private Network (VPN)

VPN adalah sebuah teknologi komunikasi yang memungkinkan terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal. Dengan menggunakan jaringan publik ini, dapat bergabung dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti ketika berada di kantor (jaringan lokal).

VPN dapat terjadi antara dua end-system atau dua PC atau bisa juga antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan encryption. Koneksi VPN juga dapat terjadi pada semua layer pada protokol OSI, sehingga dapat membuat komunikasi VPN untuk apapun kebutuhannya. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur Wide Area Network (WAN) alternative untuk mendapatkan koneksi point-to-point pribadi antara dua titik.



Gambar 2. 9 Virtual Private Network

2.8.3 SSL/TLS

Secure Socket Layer (SSL) dan Transport Layer Security (TLS), merupakan kelanjutan dari protokol cryptographic yang menyediakan komunikasi yang aman di Internet.

Secara umum SSL adalah untuk mengamankan komunikasi Web HTTP antara browser dengan web server. HTTP yang telah aman ini disebut juga HTTPS (HTTP over SSL). Contoh alamat yang menggunakan https adalah www.amazon.com, https://www.klikbca.co.id, dan lain sebagainya. HTTP bekerja pada port 80, sedangkan HTTPS bekerja pada 443 [**5**].

2.8.4 Ancaman Jaringan Komputer

Berikut beberapa ancaman yang umum ditemui pada jaringan komputer :

1. **MAC Spoofing**

Penyerang berusaha mendapatkan koneksi ke dalam jaringan dengan mengambil alamat NIC dari suatu perangkat komputer pada jaringan tersebut [**5**].

2. **ARP Spoofing**

Penyerang menangkap penyebaran paket ARP dari access point dan kemudian mengirimkan balasan ARP fiktif sehingga informasi perangkat dari penyerang akan terpetakan ke dalam tabel ARP untuk kemudian mendapatkan hak akses kedalam jaringan [**5**].

3. **Man in the Middle Attack**

Metode serangan ini biasanya didahului dengan ARP spoofing kemudian penyerang menempatkan perangkat yan g dimilikinya sebagai sebuah

komputer fiktif yang akan terlihat resmi dari sisi access point [**5**].

4. **Denial of Service**

Metode serangan dengan mengirimkan paket data dalam jumlah yang sangat besar terhadap jaringan yang menjadi targetnya secara terus-menerus. Hal ini dapat mengganggu lalu-lintas data bahkan kerusakan sistem jaringan [**5**].

2.9 Virtual Private Network (VPN)

VPN (Virtual Private Network) merupakan sebuah jaringan private yang menghubungkan Satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan Internet. Data yang dilewatkan akan diencapsulation (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya [**4**].

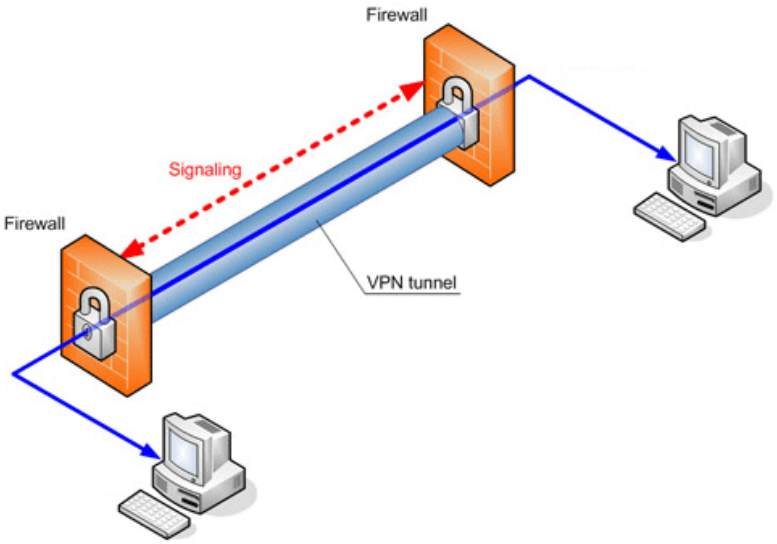
2.9.1 Pengertian VPN

Jika dibahas dari masing-masing kata dari VPN, yaitu : Virtual, Private dan Network, maka akan diperoleh arti sebagai berikut :

1. Virtual (Tidak nyata), tidak nyata, tidak tampak fisik.
2. Private (Privat), terlindungi, tidak dapat di akses dari luar
3. Network (Jaringan), sekumpulan alat-alat jaringan yang saling berkomunikasi satu dengan yang lain melalui beberapa metode arbitrary (berubah-ubah).

Sehingga dijelaskan bahwa VPN adalah fasilitas yang memungkinkan koneksi jarak jauh (remote access) menggunakan jaringan publik untuk akses ke Local Area Network (LAN) pada suatu perusahaan.

VPN merupakan suatu cara untuk membuat sebuah jaringan bersifat privat dan aman dengan menggunakan jaringan publik misalnya Internet. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara point-to-point. Data dienkapsulasi dengan header yang berisi informasi routing untuk mendapatkan koneksi point-to-point sehingga dapat melewati jaringan publik dan dapat mencapai tujuan akhir [**4**].



Gambar 2. 10 VPN Tunnel

Sedangkan untuk mendapatkan koneksi bersifat privasi, data yang dikirim harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut dengan istilah tunneling.

2.9.2 Perkembangan VPN

VPN dikembangkan untuk membangun sebuah intranet dengan jangkuan luas melalui jaringan Internet. Intranet sudah menjadi suatu komponen penting dalam suatu perusahaan saat ini. Intranet dalam perusahaan dapat berkembang sesuai dengan perkembangan perusahaan tersebut. Dengan kata lain, semakin besar suatu perusahaan maka semakin besar pula Intranet pada perusahaan tersebut. Sehingga permasalahan semakin kompleks apabila suatu perusahaan mempunyai kantor cabang dengan jarak yang jauh. Sedangkan pada pihak lain selalu berhubungan, misalnya mengirim suatu data dan sinkronisasi data [**4**].

Perkembangan Internet yang cepat menawarkan solusi untuk membangun sebuah Intranet menggunakan jaringan publik atau Internet. Di lain pihak, suatu perkembangan industri juga menuntut lima kebutuhan dalam Intranet yaitu:

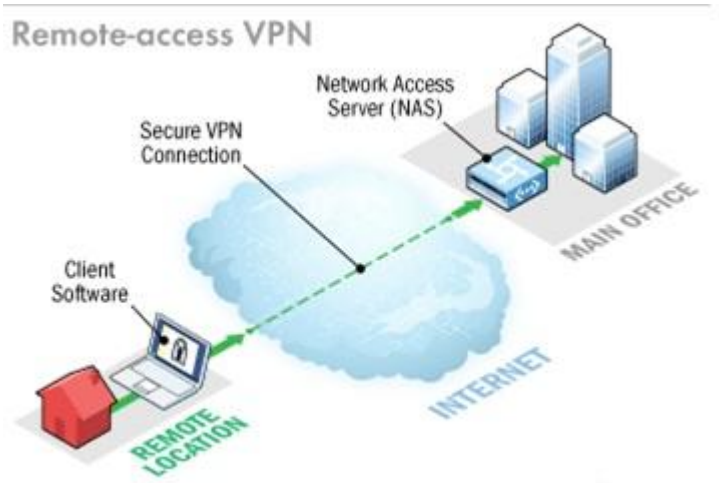
1. Kerahasiaan, yaitu kemampuan encrypt pesan sepanjang jaringan yang tidak aman.
2. Kendali akses, yaitu menentukan siapa yang diberikan akses ke jaringan dan informasi apa dan banyak orang dapat menerima.
3. Authentication, yaitu menguji identitas dari dua perusahaan yang mengadakan transaksi.
4. Integritas, yaitu menjamin bahwa file tidak berubah dalam perjalanan.
5. Non-repudiation, yaitu mencegah dua perusahaan dari menyangkal.

2.9.3 Tipe-tipe dalam VPN

Secara garis besar tipe dalam teknologi VPN yang biasa yang digunakan adalah Site-to-site dan Remote Access. Oleh karena itu,penyusun akan menjelaskan tipe-tipe tersebut [**4**].

2.9.3.1 Remote Access

Koneksi Remote Access pada VPN dibuat untuk dapat mengakses jarak jauh bagi sebuah klien. Klien Remote Access adalah pengguna komputer tunggal yang mana melakukan koneksi ke jaringan pribadi dari lokasi jarak jauh. Sebuah VPN server menyediakan akses untuk dapat mengakses sumber pada jaringan yang terkoneksi padaVPN server. Protokol yang dapat digunakan pada Remote Access adalah the Point-to-Point Tunneling Protocol (*PPTP*), Layer TwoTunneling Protocol(L2TP), Layer Two Forwarding (L2F) Protocol dan IPSec [**4**].

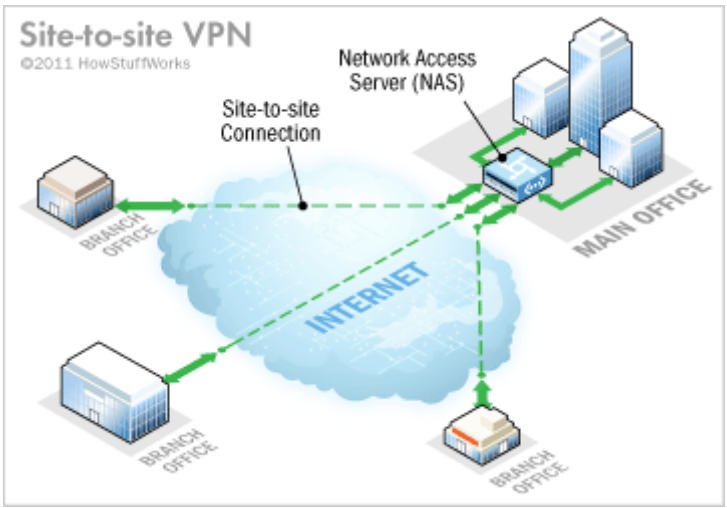


Gambar 2. 11 Tipe Remote Access

1. Poin-to-point Tunneling Protoocol (*PPTP*), yang dikembangkan dengan bantuan Microsoft, adalah suatu perluasan PPP dan terintegrasi dalam semua Microsoft sistem operasi. *PPTP* menggunakan GRE untuk encapsulation dan tunnel dapat IP, IPX, dan paket lain di Internet itu. Kerugian Yang utama adalah pembatasan yang hanya dapat satu tunnel serentak antar komunikasi.
2. Layer 2 Forwarding (L2F) dikembangkan hampir pada waktu yang sama oleh perusahaan seperti Cisco dan yang lain dan penawaran lebih berbagai kemungkinan dibanding *PPTP*, terutama mengenai pembangunan tunnel jaringan dan berbagai multipel simulasi tunnel.
3. Layer 2 Tunneling Protocol (L2Tp) diterima sebagai suatu standard industri dan digunakan secara luas oleh Cisco dan pabrikan lain. Suksesnya didasarkan pada fakta bahwa itu kombinasi keuntungan dari L2F dan *PPTP* tanpa mendapatkan kerugian. Sungguhpun itu tidak menyediakan mekanisme keamanan, dapat dikombinasikan dengan teknologi yang menawarkan mekanisme seperti seperti IPsec.
4. Layer 2 Securitty Protocol (L2Sec) dikembangkan untuk menyediakan suatu solusi pada kekurangan keamanan IPsec. Sungguhpun overheadnya agak besar, mekanisme keamanan aman digunakan, sebab sebagian besar SSL/TLS digunakan [**4**].

2.9.3.2. Site-to-Site

Site-to-site dapat juga disebut LAN-to-LAN adalah berkomunikasi antar dua atau lebih jaringan area lokal (LAN) berbeda.Suatu perusahaan pusat dengan cabangnya yang berkomunikasi dengan jarak yang berjauhan secara langsung oleh sebab itu dibangunlah VPN site-to-site sebagai solusi yang mutakhir. Bisa dibayangkan jika kantor pusat di Jakarta dan cabang di Surabaya jika dibuat jaringan lokalnya dengan menarik kabel fiber optik maka betapa besar biaya yang akan dikeluarkan. Site-to-site sering digunakan pada perusahaan kelas menengah keatas. Pada site-to-site protokol yang dapat digunakan adalah IP Security (IPsec), Generic Routing Encapsulation (GRE), the Layer Two Tunneling Protocol version 3 (L2TPv3) [**4**].



Gambar 2. 12 Type Site-to-site

2.9.4 Point to Point Tunneling Protokol (*PPTP*)

PPTP merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client (client yang berada jauh dari server) ke server pribadi perusahaan dengan membuat sebuah VPN (Virtual Private Network) melalui jaringan data berbasis TCP/IP (Snader, 2005). Protokol ini dikembangkan oleh Microsoft dan Cisco. Teknologi jaringan *PPTP* merupakan pengembangan

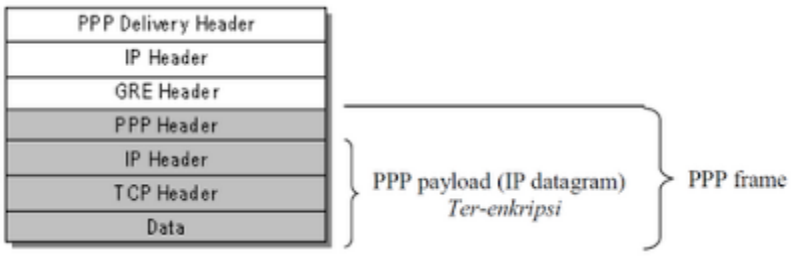
dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF) [**6**].

PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagram agar dapat ditransmisikan melalui intenet. *PPTP* juga dapat digunakan pada jaringan private LAN-to-LAN. *PPTP* terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol *PPTP* dengan aman untuk terhubung dengan private network sebagai client dengan remote access melalui internet. *PPTP* juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan *PPTP* adalah dapat digunakannya public-switched telephone network (PSTN) untuk membangun VPN. Pembangunan *PPTP* yang mudah dan berbiaya murah untuk digunakan secara luas menjadi solusi untuk remote user dan mobile user, karena *PPTP* memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet [**6**].

2.9.4.1 Karakteristik *PPTP*

Setelah *PPTP* tunnel terbentuk, data dari user ditransmisikan antara *PPTP* client dan *PPTP* server. Data yang ditransmisikan dalam bentuk IP datagram yang berisi PPP paket. IP datagram dibuat dengan menggunakan versi protokol Generic Routing Encapsulation (GRE) internet yang telah dimodifikasi. Struktur paket data yang dikirimkan melalui *PPTP* dapat digambarkan sebagai berikut [**6**]:



Gambar 2. 13 Paket data *PPTP*

2.9.4.2 Arsitektur *PPTP*

Komunikasi yang aman dibuat dengan menggunakan protokol *PPTP* secara tipikal terdiri dari tiga proses, dimana membutuhkan keberhasilan penyelesaian dari proses sebelumnya. Ketiga proses tersebut adalah :

1. PPP Connection and Communication

Suatu client *PPTP* menggunakan PPP untuk koneksi ke sebuah ISP dengan memakai line telepon standar atau line ISDN. Koneksi ini memakai protokol PPP untuk membuat koneksi dan mengenkripsi paket data [**6**].

2. *PPTP* Control Connection

Penggunaan koneksi ke internet dibuat oleh protokol PPP, protokol *PPTP* membuat control connection dari client *PPTP* ke server *PPTP* pada internet. Koneksi ini memakai TCP untuk membuat koneksi yang disebut dengan *PPTP* tunnel [**6**].

3. *PPTP* Data Tunneling

Terakhir, protokol *PPTP* membuat IP datagram yang berisi paket PPP yang terenkripsi dan kemudian dikirim melalui *PPTP* tunnel ke server *PPTP*. Server *PPTP* memeriksa IP datagram dan mendekripsi paket PPP, dan kemudian mengarahkan paket yang terdekripsi ke jaringan private [**6**].

2.9.4.3 Keamanan *PPTP*

PPTP secara luas memberikan layanan keamanan otentikasi dan enkripsi yang kuat dan tersedia pada computer yang menjalankan *remote access server*(RAS) dari server Windows NT versi 4.0 dan Windows NT Workstation versi 4.0 ke client *PPTP* di internet. *PPTP* juga dapat melindungi server *PPTP* dan jaringan private dengan mengabaikan semuanya kecuali *PPTP* traffic. Walaupun kemanannya kuat, *PPTP* sangat mudah digunakan dengan adanya firewalls [**6**].

1. Otentikasi

Otentikasi dibutuhkan server network access ISP dalam initial dial-in. Jika otentikasi ini dibutuhkan maka sangat sulit untuk log on ke server network access ISP; otentikasi ini tidak berhubungan dengan otentikasi berbasis Windows NT. Dengan kata lain, jika server windows NT versi 4.0 sebagai server *PPTP*, maka server tersebut yang akan mengendalikan semua akses ke jaringan private. Dengan kata lain, server *PPTP* merupakan gateway menuju jaringanprivate. Server *PPTP* membutuhkan proses logon berbasis Windows NT standar. Semua client *PPTP* harus memiliki user name dan password. Oleh karena itu keamanan logon akses terbatas dengan menggunakan komputer dengan Windows NT server atau windows NT workstation versi 4 harus sama dengan keamanan saat logging pada komputer berbasis windows NT yang terkoneksi ke LAN lokal. Otentikasi client remote *PPTP* dilakukan dengan menggunakan metode otentikasi PPP yang sama dimana client RAS langsung terhubung dengan server RAS. User account terletak dalam directory service windows NT server versi 4.0 dan diatur melalui user manager untuk domain. User manager ini menyediakan pengaturan terpusat yang terintegrasi dengan user account jaringan private yang tersedia. Hanya account yang diakui saja yang bisa mengakses jaringan. Memiliki password yang sulit ditebak akan mengurangi resiko terhadapbrute force attack karena proses otentikasi tersebut rentan terhadap brute force attack.

2. Access Control

Setelah proses otentikasi, semua akses ke private LAN diteruskan dengan memakai model keamanan berbasis windows NT. Akses ke sumber pada drive NTFS atau sumber jaringan lainnya membutuhkan ijin yang sesuai. Direkomendasikan bahwa sistem file NTFS digunakan untuk sumber file yang diakses oleh client *PPTP* [**6**].

3. Enkripsi Data

Untuk enkripsi data, *PPTP* menggunakan proses enkripsi RAS "shared-secret". Disebut "shared-secret" karena pada awal dan akhir koneksi *PPTP* membagi kunci enkripsi. Dalam implementasi Microsoft dari RAS, shared secret disebut user password. (metode enkripsi lainnya berbasis enkripsi pada tersedianya kunci untuk public; metode enkripsi kedua ini dikenal sebagai public key encryption). *PPTP* menggunakan skema PPP encryption dan PPPcompression. CCP (Compression Control Protocol) digunakan PPP untuk enkripsi. User namedan password *PPTP* client tersedia untuk *PPTP* server dan diberikan oleh *PPTP* client. Kunci enkripsi dihasilkan dari penyimpanan password yang telah di-hash yang terdapat di client dan server. RSA RC4 standar digunakan untuk menghasilkan session key 40 bit berdasarkan padapassword client. Kunci ini dipakai untuk mengenkripsi semua data yang melewati internet, untuk melindungi koneksi private agar aman.

Data pada paket-paket PPP dienkripsi. Paket PPP yang berisi blok data terenkripsi kemudian dibungkus hingga manjadi IP datagram yang besar untuk routing melalui internet ke server*PPTP*. Jika hacker internet melakukan intercept IP datagram, ia hanya akan mendapatkan media header, IP header dan paket PPP berisi blok data yang terenkripsi bukan data yang terdekripsi.

Hal ini akan melindungi semua paket yang berasal dari server *PPTP* dan jaringan private. Berhubungan dengan enkripsi PPP, maka hal ini akan menjamin hanya data terenkripsi yang berhak masuk dan keluar private LAN.

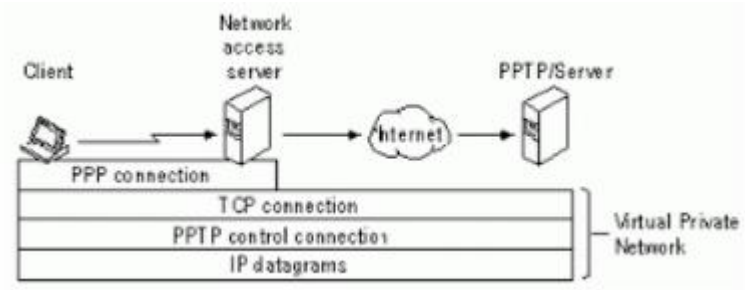
2.9.4.4 Cara Kerja *PPTP*

Cara kerja *PPTP* dimulai dari sebuah remote atau *PPTP* client mobile yang membutuhkan akses ke sebuah LAN private dari sebuah perusahaan. Pengaksesan dilakukan dengan menggunakan ISP lokal. Client (yang menggunakan Windows NT Server versi 4.0 atau Windows NT Workstation versi 4.0) menggunakan Dial-Up networking dan protokol remote access PPP untuk terhubung ke sebuah ISP [**6**].

Client terhubung ke Network Access Server (NAS) pada fasilitas ISP. NAS di sini bisa berupa prosesor front-end, server dial-in atau server Point-of-Presence (POP). Begitu terhubung, client bisa mengirim dan menerima paket data melalui internet. NAS menggunakan protocol TCP/IP untuk semua trafik yang melalui internet.

Setelah client membuat koneksi PPP ke ISP, panggilan Dial-Up Networking yang kedua dibuat melalui koneksi PPP yang sudah ada. Data dikirimkan menggunakan koneksi yang kedua ini dalam bentuk IP datagram yang berisi paket PPP yang telah ter-enkapsulasi.

Panggilan yang kedua tersebut selanjutnya menciptakan koneksi VPN ke server *PPTP* pada LAN private perusahaan. Koneksi inilah (melalui panggilan kedua) yang di-istilahkan sebagai tunnel (lorong). Berikut ini gambar yang menjelaskan proses tersebut:



Gambar 2. 14 Tunnel *PPTP*

Tunneling pada gambar 2.5 adalah sebuah proses pengiriman paket data ke sebuah komputer pada jaringan privat dengan me-routing paket data tersebut melalui beberapa jaringan yang lain, misalnya Internet. Router-router jaringan yang lain tidak bisa mengakses komputer yang berada pada jaringan privat. Oleh karena itu, tunneling memungkinkan jaringan routing untuk mentransmisikan paket data ke komputer penghubung, seperti *PPTP* server, yang terhubung ke jaringan routing dan jaringan privat. *PPTP* client dan *PPTP* server menggunakan tunneling untuk merutekan paket data secara aman ke komputer yang berada pada

jaringan privat melalui router-router yang hanya mengetahui alamat server penghubung jaringan privat [**6**].

2.10 Mikrotik

Mikrotik adalah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia, pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully yang berkebangsaan Amerika Serikat berimigrasi ke Latvia dan berjumpa Arnis yang sarjana Fisika dan Mekanika di sekitar tahun 1995. Tahun 1996 John dan Arnis mulai me-routing dunia (visi Mikrotik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS DOS yang dikombinasikan dengan teknologi Wireless LAN (W-LAN) Aeronet berkecepatan 2Mbps di Moldova, tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia, karena ambisi mereka adalah membuat satu peranti lunak router yang handal dan disebarkan ke seluruh dunia. Ini agak kontradiksi dengan informasi yang ada di web Mikrotik, bahwa mereka mempunyai 600 titik (pelanggan) wireless dan terbesar di dunia [**7**].

Prinsip dasar mereka bukan membuat Wireless ISP (WISP), tapi membuat program router yang handal dan dapat dijalankan di seluruh dunia. Latvia hanya merupakan “tempat eksperimen” John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar empat ratusan pelanggannya.

Mikrotik mempunyai 2 produk antara lain Mikrotik OS dan Mikrotik Routerboard.

1. MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti

merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

2. Mikrotik RouterBoard adalah router embedded produk dari mikrotik. Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan os RouterOS yang berfungsi sebagai router jaringan, bandwidth management, proxy server, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server.

2.10.1 Fungsi Mikrotik

Fungsi utama mikrotik adalah menjadikan sebuah komputer sebagai network router (Routing).Selain itu, mikrotik juga mempunyai fungsi untuk menjalankan aplikasi, meliputi [**7**]:

- Aplikasi kapasitas akses *Bandwith Management*
- Aplikasi *Firewall*
- Wireless Access Point (Wi-Fi),
- Aplikasi Backhaul Link,
- Sistem *Hotspot*
- Virtual Private Netword (VPN) Server,
- dll.

2.10.2 Fitur – fitur Mikrotik

1. Penanganan Protokol TCP/IP [**7**]:
   - **Firewall and NAT** - stateful packet filtering; Peer-to-Peer protocol filtering; source and destination NAT; classification by source MAC, IP addresses, ports, protocols, protocol options, interfaces, internal marks, content, matching frequency.
   - **Routing** - Static routing; Equal cost multi-path routing; Policy based routing (classification by source and destination addresses and/or by firewall mark); RIP v1 / v2, OSPF v2, BGP v4.
   - **Data Rate Management** - per IP / protocol / subnet / port / firewall mark; HTB, PCQ, RED, SFQ, byte limited queue, packet limited queue;

hierarchical limitation, CIR, MIR, contention ratios, dynamic client rate equalizing (PCQ) .

- **HotSpot** - HotSpot Gateway with RADIUS authentication/accounting; data rate limitation; traffic quota; real-time status information; walled-garden; customized HTML login pages; iPass support; SSL secure authentication.
- **Point-to-Point tunneling protocols** - *PPTP*, PPPoE and L2TP Access Concentrators and clients; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; MPPE encryption; compression for PPPoE; data rate limitation; PPPoE dial on demand.
- **Simple tunnels** - IPIP tunnels, EoIP (Ethernet over IP)
- **IPsec - IP security AH and ESP protocols**; Diffie-Hellman groups 1,2,5; MD5 and SHA1 hashing algorithms; DES, 3DES, AES-128, AES-192, AES-256 encryption algorithms; Perfect Forwarding Secresy (PFS) groups 1,2,5 .
- **Web proxy - FTP, HTTP and HTTPS caching proxy server**; transparent HTTP caching proxy; SOCKS protocol support; support for caching on a separate drive; access control lists; caching lists; parent proxy support.
- **Caching DNS client - name resolving for local use**; Dynamic DNS Client; local DNS cache with static entries.
- **DHCP - DHCP server per interface**; DHCP relay; DHCP client; multiple DHCP networks; static and dynamic DHCP leases.
- **Universal Client** - Transparent address translation not depending on the client's setup.
- **VRRP - VRRP** protocol for high availability.
- **UPnP** - Universal Plug-and-Play support.
- **NTP** - Network Time Protocol server and client; synchronization with GPS system.

- **Monitoring/Accounting** - IP traffic accounting, firewall actions logging.
- **SNMP** - read-only access.
- **M3P** - MikroTik Packet Packer Protocol for Wireless links and Ethernet.
- **MNDP** - MikroTik Neighbor Discovery Protocol; also supports Cisco Discovery Protocol (CDP) .
- **Tools** - ping; traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer.

2. Layer 2 konektivitas :

- **Wireless** - IEEE802.11a/b/g wireless client and Access Point; Wireless Distribution System (WDS) support; virtual AP; 40 and 104 bit WEP; access control list; authentication on RADIUS server; roaming (for wireless client); Access Point bridging.
- **Bridge** - spanning tree protocol; multiple bridge interfaces; bridge firewalling.
- **VLAN** - IEEE802.1q Virtual LAN support on Ethernet and WLAN links; multiple VLANs; VLAN bridging.
- **Synchronous** - V.35, V.24, E1/T1, X.21, DS3 (T3) media types; sync-PPP, Cisco HDLC, Frame Relay line protocols; ANSI-617d (ANDI or annex D) and Q933a (CCITT or annex A) Frame Relay LMI types.
- **Asynchronous** - serial PPP dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; onboard serial ports; modem pool with up to 128 ports; dial on demand.
- **ISDN** - ISDN dial-in / dial-out; PAP, CHAP, MSCHAPv1 and MSCHAPv2 authentication protocols; RADIUS authentication and accounting; 128K bundle support; Cisco HDLC, x75i, x75ui, x75bui line protocols; dial on demand.
- **SDSL** - Single-line DSL support; line termination and network termination modes.

2.10.3 Level Mikrotik dan Kemampuan

Mikrotik Router hadir dalam berbagai level. Tiap level memiliki kemampuannya yang berbeda-beda., diantaranya [**7**]:

- Level 0 (gratis). Tidak membutuhkan lisensi untuk menggunakannya dan penggunaan fitur hanya dibatasi selama 24 jam setelah instalasi dilakukan.
- Level 1 (demo). Dapat digunakan sebagai fungsi routing standar saja dengan 1 pengaturan serta tidak memiliki limitasi waktu untuk menggunakannya.
- Level 3. Mencakup level 1 ditambah dengan kemampuan untuk menajemen router berinterface ethernet.
- Level 4. Mencakup level 1 dan 3 ditambah dengan kemampuan untuk mengelola wireless client atau serial interface, untuk aplikasi hotspot bisa digunakan untuk 200 pengguna.
- Level 5. Mencakup level 1, 3 dan 4 ditambah dengan kemampuan wireless AP, untuk aplikasi hotspot bisa digunakan untuk 500 pengguna.
- Level 6. Mencakup semua level dan tidak memiliki limitasi apapun, untuk aplikasi hotspot bisa digunakan untuk pengguna yang tidak terbatas.

Tabel 2. 2 Tabel Level Mikrotik

Level number	1 (DEMO)	3 (ISP)	4 (WISP)	5 (WISPAP)	6 (Controller)
Wireless Client and Bridge	-	-	yes	yes	yes
Wireless AP	-	-	-	yes	yes
Synchronous interfaces	-	-	yes	yes	yes
EoIP tunnels	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	1	200	200	500	unlimited
PPTP tunnels	1	200	200	unlimited	unlimited
L2TP tunnels	1	200	200	unlimited	unlimited
VLAN interfaces	1	unlimited	unlimited	unlimited	unlimited
P2P firewall rules	1	unlimited	unlimited	unlimited	unlimited
NAT rules	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	1	1	200	500	unlimited
RADIUS client	-	yes	yes	yes	yes
Queues	1	unlimited	unlimited	unlimited	unlimited
Web proxy	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	-	yes	yes	yes	yes
Upgrade	configuration erased on upgrade	yes	yes	yes	yes

2.10.4 Produk Mikrotik

Saat ini produk-produk Mikrotik sudah lebih berfariasi.

Berikut merupakan produk dari mikrotik [**7**]:

1. DOM

Berbentuk media penyimpanan seperti hardisk dari beberapa vendor yang sudah ada di Indonesia yang berisikan Mikrotik OS sekaligus dengan lisensinya.



Gambar 2. 15 DOM Mikrotik

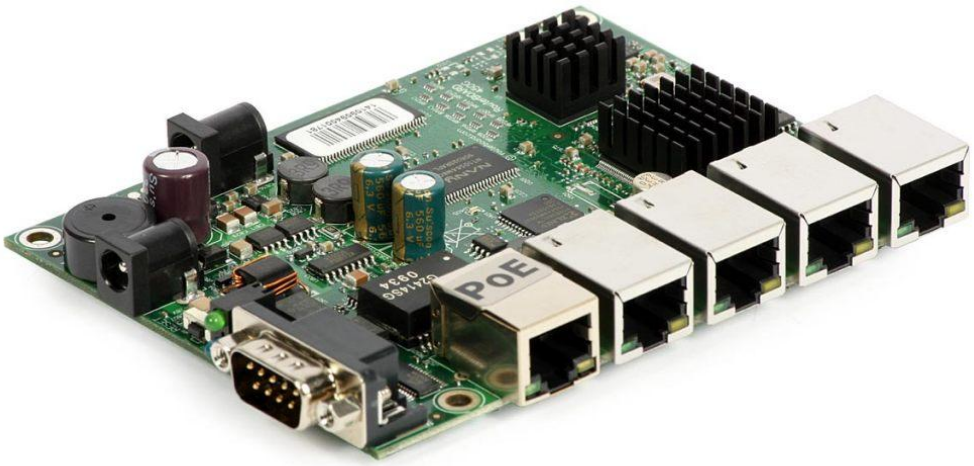
2. Routerboard

Routerboard adalah router embedded produk dari mikrotik. routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboardmenggunakan os RouterOS fungsinya sebagai router jaringan, bandwidth management, proxy server, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server.

Ada beberapa seri routerboard yang juga bisa berfungsi sebagai wifi. sebagai wifi access point, bridge, wds ataupun sebagai wifi client. seperti seri RB411, RB433, RB600. dan sebagian besar isp wireless menggunakan routerboard untuk menjalankan fungsi wirelessnya baik sebagai ap ataupun client [**7**].

Dengan routerboard kita bisa menjalankan fungsi sebuah router tanpa tergantung pada pc lagi. karena semua fungsi pada router sudah ada dalam

routerboard. dibandingkan dengan pc yang diinstal routerOS, routerboard ukurannya lebih kecil, lebih kompak dan hemat listrik karena hanya menggunakan adaptor. untuk digunakan di jaringan wifi bisa dipasang diatas tower dan menggunakan PoE sebagai sumber arusnya [**7**].



Gambar 2. 16 Routerboard Mikrotik

2.11 Tunneling

Tunneling merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung. Disebut tunnel atau saluran karena aplikasi yang memanfaatkannya hanya melihat dua end point atau ujung, sehingga paket yang lewat pada tunnel hanya akan melakukan satu kali lompatan atau hop. Data yang akan ditransfer dapat berupa frame atau paket dari protocol yang lain. Protocol tunneling tidak mengirimkan frame sebagaimana yang dihasilkan oleh node asalnya begitu saja, melainkan membungkusnya men-enkapsulasi dalam header tambahan. Header tambahan tersebut berisi informasi routing sehingga data frame yang dikirim dapat melewati jaringan internet. Jalur yang dilewati data dalam internet disebut tunnel [**4**].

Saat data tiba pada jaringan tujuan, proses yang terjadi selanjutnya adalah dekapsulasi, kemudian data original akan dikirim ke penerima terakhir.Tunneling mencangkup keseluruhan proses mulai dari enkapsulasi,

transmisi dan dekapsulasi. Sesuai dengan arti tunnel, dalam membentuk suatu VPN ini dibuat suatu tunnel didalam jaringan public untuk menghubungkan antara jaringan yang satu dan jaringan yang lain dari suatu group yang akan membangun VPN tersebut. Seluruh komunikasi data antar jaringan pribadi akan melalui tunnel ini, sehingga user dari jaringan public yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Metode tunneling yang umum digunakan :

1. IPX to IP Tunneling
2. PPP to IP Tunneling

2.11.1 Standart dari Tujuan Tunneling

General Routing Encapsulation (GRE) menyediakan standard untuk pembangunan tunnel data, yang digambarkan di tahun 1994 di Request for Comments (RFC) 1701 dan 1702. Barangkali, karena definisi ini tidak merupakan suatu definisi protokol, tetapi kurang lebih suatu proposal standard pada bagaimana cara data tunnel, implementasi ini telah menemukan caranya dalam banyak alat dan menjadi basis untuk protokol lain [**4**].

Konsep GRE adalah sederhana. Suatu protokol header dansuatu penyerahan header ditambahkan pada paket asli dan muatan penghasil untungnya adalah encapsulasi dalam paket yang baru itu. Tidak ada encryption dilaksanakan.

Keuntungan dari model ini hampir dipastikan menawarkan banyak berbagai kemungkinan, ketransparanan memungkinkan penerus dan pengurus untuk melihat di dalam paket dan keputusan yang didasarkan pada jenis pengiriman muatan penghasil.

Ada banyak implementasi untuk GRE yang membangun software tunnel di bawah Linux; hanya kernal yang sangat penting, yang mana dipenuhi oleh distribusi paling modern

2.11.1.1 Implementasi Protokol pada Layer2

Paket encapsulasi pada OSI Lapisan 2 mempunyai suatu keuntungan penting tunnel bisa memindahkan protokol non-IP. IP adalah suatu standard yang digunakan secara luas dalam Internet dan dalam Ethernet jaringan.

Bagaimanapun, ada standard yang berbeda juga. Sistem Netware, sebagai contoh, menggunakan

Internetwork Packet Exchange (IPX) protokol untuk komunikasi. VPN teknologi yang terdapat pada Lapisan 2 secara teoritis banyak jenis tunnel. Dalam banyak kasus, sebenarnya suatu Point-To-Point Protokol (PPP) memutuskan alat yang mana digunakan untuk menghubungkan pada tunnel yang endpoint [**4**].

2.12 Cygwin

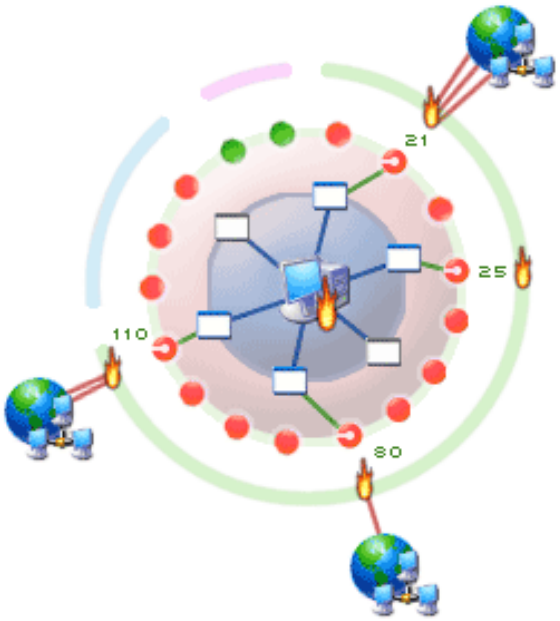
Cygwin adalah port dari tool pengembangan GNU (GNU's Not UNIX) untuk Microsoft Windows. Hal ini dimungkinkan dengan adanya library Cygwin sebagai penyedia sistem dan lingkungan UNIX yang dibutuhkan oleh tool GNU tersebut.Singkatnya, Cygwin adalah sebuah lingkungan yang menyerupai Linux untuk Windows. Cygwin terdiri dari dua komponen:

- Sebuah DLL (cygwin.dll) yang berperan sebagai emulasi Linux API dan berperan menyediakan fungsionalitas Linux API yang penting.
- Sebuah kumpulan tool, yang memberikan nuansa dan tampilan seperti Linux.

Dengan terinstalnya tool-tool semacam ini, memungkinkan untuk dibuat konsol Win32 atau aplikasi GUI yang menggunakan standar Microsoft Win32 API dan/atau Cygwin API. Hasilnya, banyak program penting Unix yang dapat digunakan di Windows tanpa membutuhkan perubahan penting dari kode sumbernya. Ini termasuk mengkonfigurasi dGNU (termasuk paket tool pengembangan Cygwin) [**8**].

2.13 Port Knocking

Di dalam firewall semua komunikasi yang keluar dan masuk dikontrol. Port yang tidak penting dapat diblokir (ditutup) dan port yang penting dan berbahaya juga dapat diblokir, sehingga hanya pihak yang diijinkan saja yang boleh masuk melalui port tersebut [**9**].



Gambar 2. 17 Penutupan port

Cara ini merupakan sistem pengamanan jaringan komputer yang paling efektif dan banyak digunakan. Akan tetapi terkadang pemblokiran yang dilakukan sering menjadi tidak fleksibel, ketika dibutuhkan untuk menjalin komunikasi dengan apa yang ada di dalam jaringan, firewall tidak mengijinkannya karena mungkin memang berada pada area yang tidak diijinkan. Padahal komunikasi yang ingin dilakukan sangatlah penting untuk kelancaran kerja. Misalnya melakukan koneksi dengan internet dan butuh mengakses web server melalui SSH untuk memperbaiki konfigurasinya, sementara port SSH pada server tersebut dilarang untuk diakses dari internet oleh firewall, tentu hal ini akan sangat merepotkan. Untuk menghindari hal-hal semacam ini, ada suatu metode yang sangat efektif yaitu dengan menggunakan metode port knocking. Port knocking adalah suatu metode untuk membangun komunikasi antar komputer dari mana pun selama masing-masing komputer tersebut terhubung dalam suatu jaringan komputer, dengan perangkat komputer yang tidak membuka port komunikasi apapun secara bebas, tetapi perangkat tersebut masih tetap dapat diakses dari luar, dengan menggunakan suatu format konfigurasi port ketukan yang berupa percobaan untuk mengirimkan koneksi pada port ketukan [**9**].

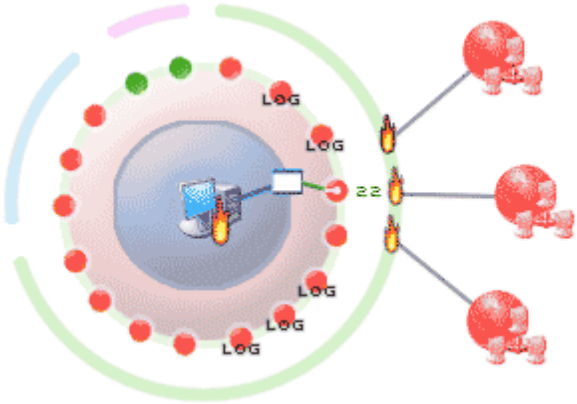
2.12.1 Manfaat Port Knocking

Jika dilihat sesaat, Port Knocking memang tidak terlalu banyak gunanya dan tidak terlalu istimewa. Hanya melakukan buka tutup port komunikasi saja tentu tidaklah terlalu banyak gunanya bagi pengguna jaringan lokal. Namun bagi para pekerja telekomuter, para pengguna komputer yang sering bekerja di luar kantor atau para administrator jaringan dan server yang harus mengurusi server-server mereka 24 jam dari mana saja, Port Knocking merupakan metode yang luar biasa sebagai sebuah jalan penghubung ke perangkat-perangkat komputer mereka. Port knocking cocok untuk mereka yang masih ingin memperkuat sistem keamanan komputer dan perangkat jaringannya, sementara tetap pula ingin memiliki koneksi pribadi ke dalamnya secara kontinyu dan dapat dilakukan dari mana saja. Komunikasi pribadi maksudnya koneksi yang tidak terbuka untuk umum seperti SMTP atau HTTP. Biasanya komunikasi pribadi ini lebih bersifat administratif dan menggunakan servis-servis seperti telnet, SSH, FTP, TFTP, dan banyak lagi. Komunikasi pribadi ini akan sangat berbahaya jika dapat juga dilakukan oleh orang lain yang tidak berhak. Dengan menggunakan Port knocking, servis-servis tersebut akan tetap tertutup untuk diakses oleh publik, namun masih dapat secara fleksibel di buka oleh siapa saja yang memiliki kombinasi ketukan port-nya [**10**].

2.12.2 Cara Kerja Port Knocking

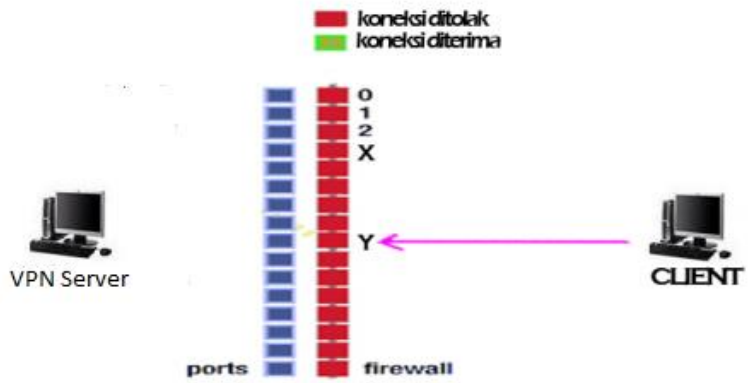
Port knocking bekerja seperti halnya brankas dengan kunci kombinasi angka putar. Pada brankas tersebut, Anda diharuskan memutar kunci kombinasi beberapa kali hingga tepat seperti yang ditentukan. Sebenarnya Anda memutar lapisan-lapisan kunci di dalam brangkas. Dalam lapisan-lapisan kunci tersebut terdapat sebuah lubang kunci. Jika sebuah putaran tepat, maka sebuah lubang terbuka. Jika seluruh putaran dilakukan dengan kombinasi yang benar, maka seluruh lubang terbuka dan menciptakan sebuah jalur khusus yang bebas tidak ada hambatan sama sekali. Jalur lubang kunci tadi tidak lagi menjadi penghalang pintu brankas untuk dibuka, sehingga pintu dapat terbuka dengan mudah. Port knocking juga menggunakan sistem yang hampir sama, yaitu menggunakan kombinasi lapisan-lapisan kunci untuk dapat mengamankan sebuah port komunikasi.

Perbedaannya ada pada lapisan kunci yang digunakannya. Kunci dari sistem port knocking adalah port- port komunikasi itu sendiri. Cara membuka kuncinya adalah dengan mengakses dengan sengaja beberapa port komunikasi yang memang tertutup. Ketika beberapa port komunikasi tadi diakses dengan kombinasi tertentu, maka akan terbuka sebuah port komunikasi baru yang bebas anda masuki [**10**].

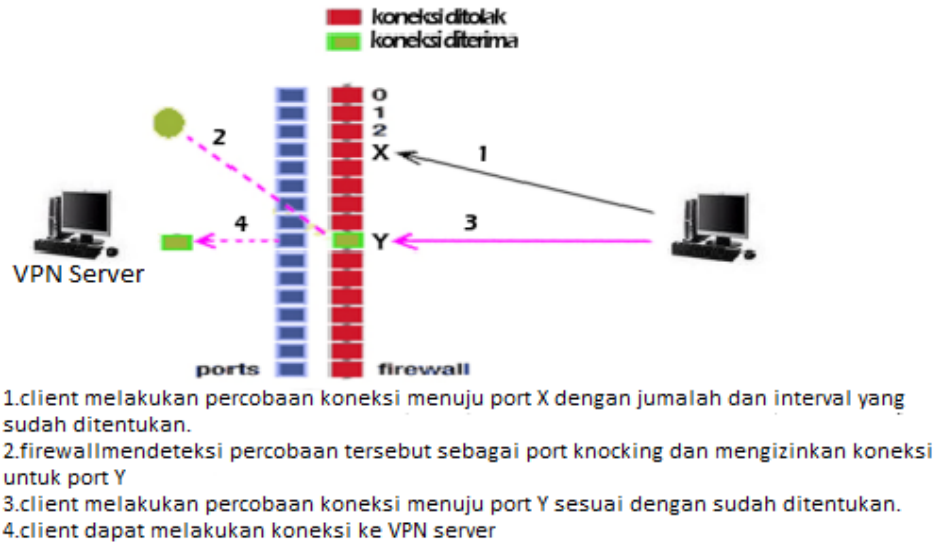


Gambar 2. 18port yang dilindungi port knocking

Sebagai contoh, untuk membuka port 22 yang merupakan port komunikasi untuk aplikasi remote login SSH, Anda diharuskan “mengetuk” port 450, 360, 270, 180. Ketika kombinasinya benar dalam suatu waktu tertentu, maka akan terbuka port 22 yang Anda inginkan. Sistem seperti ini dapat tercipta dengan bantuan sebuah program firewall. Program firewall biasanya memiliki fasilitas untuk melakukan logging terhadap setiap proses komunikasi yangkeluar-masuk melaluinya. Dari membaca log inilah, sistem Port knocking dapat mengetahui kombinasi ketukan. Ketika sistem Port knocking membaca sebuah kombinasi yang tepat pada log, maka sebuah proses otomatis menjalankan aplikasi yang akan membuka port komunikasi yang ditentukan. Setelah terbuka, maka jadilah sebuah pintu masuk kedalam perangkat Anda [**10**].



Gambar 2. 19 Koneksi ditolak



Gambar 2. 20 Koneksi diterima

2.12.3 Pengimplementasian Port Knocking

Penerapan atau pengimplementasian port knocking bisa diimplementasikan pada beberapan perangkat atau operating sistem yang menyediakan fitur atau service firewall contoh nya Linux maupun Operating system yang berbasis UNIX.

Port Knocking pada dasar nya dapat di implementasi kan dengan meng custom rule-rule firewall yang terdapat pada masing-masing perangkat atau

Operating sistem. Pengimplementasian port knocking pada operating sistem berbasis Linux atau UNIX , karena selain open source rule-rule firewall yang terdapat pada operating sistem tersebut dapat dimodifikasi dirombak sedemikan rupa agar pemanfaatan firewallpun lebih efektif sesuai dengan kepentingan.