BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Rujukan penelitian yang pertama yaitu Jurnal Hambali mahasiswa STMIK Royal pada tahun 2018 dengan judul membangun *blocking* situs menggunakan web proxy.dalam penelitiannya peneliti menggunakan mikrotik winbox yaitu untuk memblokir situs pada internet yang tidak boleh akses oleh server tersebut untuk itu perlu dilakukan upaya pencegahan terhadap informasi negatif. Melakukan proses blokir terhadap situs tertentu (pornografi, kekerasan, jejaring sosial, perjudian) mutlak perlu dilakukan untuk menghindarkan dari pengguna yang tidak berhak. Blocking situs tersebut menggunakan web proxy mikrotik os rb750 yang mudah dan murah dibanding dengan router lain

Rujukan penelitian yang kedua yaitu Armanto mahasiswa Sekolah Tinggi Manajemen dan Ilmu Komputer Musi Rawas pada tahun 2017 dengan judul *Blocking* situs di Router Mikrotik RB 2011 dengan menggunakan web proxy (studi kasus STIE-Musi Rawas Lubuk Linggau). Dalam penelitannya peneliti menggunakan mikrotik winbox yaitu untuk memblokir situs pada internet yang tidak boleh akses ke server tersebut oleh karena itu dengan adanya pemblokiran situs ini Mahasiswa ataupun tenaga pendidik dan tenaga kependidikan tidak bisa membuka situs negatif lagi dikarenakan situs sudah terblokir dengan menggunakan mikrotik os yang dirancang untuk memblokir situs situs yang dianggap negtive dan dilekapai dengan fitur router yang sangat efektif untuk pemblokiran situs dan pengamanan jaringan.

Sedangkan penelitian yang akan dilakukan oleh penelitian tidak jauh berbeda dengan penelitian sebelumnya yaitu untuk memblokir situs menggunakan web proxy agar mahasiswa dijurusan Teknik Komputer ini tidak bisa membuka situs yang dilarang oleh server tersebut dikarenakan tidak bermanfaat bagi mahasiswa di jurusan Teknik Komputer

Untuk lebih jelas dan detail terhadap penelitian terdahulu dapat dilihat pada table berikut:

Tabel 2.1 Perbandingan Penelitian Terdahuliu dengan Penelitian Sekarang

No	Penelitian	Persamaan	Perbedaan
1.	Hambali. Membangun blocking situs	- Memblokir situs menggunakan web proxy	- Pemblokiran situs ini hanya digunakan di

	menggunakan web proxy mikrotik RB 750.	- Untuk itu perlu dilakukan upaya pencegahan terhadap informasi negatif. Melakukan proses blokir terhadap situs tertentu	jurusan Teknik computer politeknik negeri sriwjaya - Penulis menggunakan aplikasi mikrotik winbox versi 3.19 sedangkan peneliti menggunakan mikrotik router versi 6.3
2.	Armanto. *Blocking* situs di Router Mikrotik RB 2011 dengan menggunakan web proxy (studi kasus STIE-Musi Rawas Lubuk Linggau)	- Pada penelitian ini menggunakan beberapa alat untuk mendukung penelitian ini seperti satu unit router mikrotik rb 2011 yang digunkan sebagai server jaringan,satu buah laptop untuk melakuan pengaturan pada router, satu buah swich untuk pembagian jaringan	- Pemblokiran situs ini hanya digunakan di jurusan Teknik computer politeknik negeri sriwjaya - Penulis menggunakan aplikasi mikrotik winbox versi 3.19 sedangkan peneliti menggunakan mikrotik router versi 6.3

2.2 Personal Computer

Menurut Khairil (2012) Pengertian Personal Komputer Istilah komputer (computer) berasal dari bahasa latin *computare* yang berart menghitung. Komputer mempunyai arti yang sangat luas dan berbeda untuk orang yang berbeda. Berikut ini definisi komputer yang didapat dari beberapa buku komputer.

Menurut (Robert H. Blissmer), Komputer adalah suatu alat elektronik yang mampu melakukan beberapa tugas sebagai berikut:

1. Menerima input.
2. Memproses input sesuai dengan programnya.
3. Menyimpan perintah-perintah dan hasil dan pengolahan.
4. Menyediakan output dalam bentuk informasi.

Menurut buku (Donald H. Sanders), komputer adalah sistem elektronik untuk manipulasi data yang cepat dan tepat serta

2.3 Pengertian Internet

Menurut Khairil (2012) Pengertian Personal Komputer**,** Internet adalah singkatan dari *Interconnection Networking*. Berasal dari bahasa latin "inter" berarti antara. Secara kata perkata INTERNET berarti jaringan antara atau penghubung, sehingga definisi internet ialah hubungan antara berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasi maupun aplikasinya dimana hubungan tersebut memanfaatkan kemajuan komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi yaitu protokol TCP/IP atau *Transmission Control/Internet Protocol*

2.4 Mikrotik *Router OS*

Menurut Sujalwo (2011) *Mikrotik RouterOS™,* merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk mem berikan kemudahan bagi penggunanya. Adminis trasinya bisa dilakukan melalui *Windows application* (WinBox). Selain itu insta lasi dapat dilakukan pada sebuah *Personal Computer* (PC). PC yang akan dijadikan router mikrotik pun tidak memerlukan *resource* yang cukup besar untuk penggunaan

Mikrotik dibuat oleh MikroTikls sebuah perusahaan di kota Riga, Latvia. Awalnya, mikrotik ditujukan untuk perusahaan jasa layanan Internet (PJI) atau *Internet Service Provider* (ISP) yang melayani pelanggannya menggunakan teknologi nirkabel atau *wireless.* Saat ini *MikroTikls* memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet dibanyak negara di dunia. MikroTik sekarang menyediakan *hardware* dan *software* untuk konektivitas internet di sebagian besar negara di seluruh dunia. Produk *hardware* unggulan Mikrotik berupa *Router, Switch*, *Antena,* dan perangkat pendukung lainnya. Produk *Software* unggulan *Mikrotik* adalah *MikroTik RouterOS.*

2.5 Web Proxy dan NAT

Menurut Wijayanta, Setya (2013) Web *Proxy* adalah website berbasis *proxy server* yang bertindak sebagai perantara untuk menerima / melakukan *request* terhadap kontent dari sebuah jaringan internet atau intranet. *Proxy server* bertindak sebagai *gateway* untuk setiap komputer klien. *Web Server* yang menerima permintaan dari *web proxy* akan menerjemahkannya, dan seolah-olah permintaan tersebut langsung dari komputer *clien*. Dan dalam proses pengiriman data, ip address tidak terdeteksi karena telah disembunyikan terlebih dahulu oleh *proxy.*

Jika menggunakan *web proxy* kita dapat menghemat *bandwidth* dan menambah kecepatan pada saat *browsing* internet karena *web proxy* mempunyai kemampuan untuk menyimpan data

ke *storage local* sehingga jika ada *client* lain yang membuka situs yang sama, maka isi *website* sebagian besarnya di ambil dari *storage local server* selain itu juga *web proxy* mempunyai kemampuan untuk memblokir situs terlarang, seperti situs judi ataupun pornografi.

Karena jika menggunakan NAT, maka Mikrotik hanya akan meneruskan HTTP Request yang dibuat oleh komputer I. HTTP request tersebut diteruskan ke ioleh Mikrotik tanpa membuat HTTP *request* baru seperti halnya pada *Web Proxy*.

NAT hanya menangani paket data saja, sedangkan *Proxy* bekerja dengan memeriksa konten dari HTTP *Request dan Response* secara detail, sehingga *Proxy* sering juga disebut sebagai *Application Firewall*.

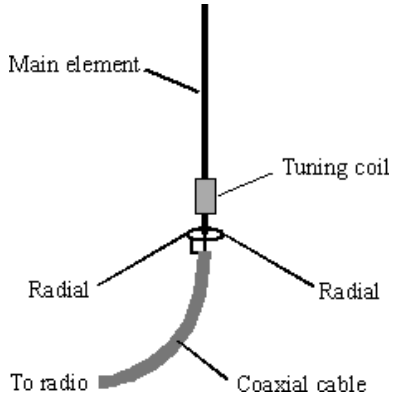
2.6 *Access Point*

Menurut Titahningsih, Prastise (2018) *Access point* adalah suatu perangkat jaringan komputer yang dapat menghubungkan peranti nirkabel dengan jaringan lokal memakai *wifi, bluetooth, wireless,* dan lain-lain. Biasanya *access point* menggunakan *router, hub atau switch* sebagai perangkat keras untuk menghubungkan peranti nirkabel dengan jaringan lokal yang telah dibuat oleh administrator. Perangkat *access point* ini memiliki antena dan transceiver yang digunakan sebagai penerima dan penyebar sinyal untuk dihubungkan dengan peranti yang terhubung dengan *access point.* Untuk terhubung dengan *access point*, pemilik perangkat biasanya diharuskan untuk memasukkan password yang sudah dibuat oleh administrator jaringan atau pembuat *access point*

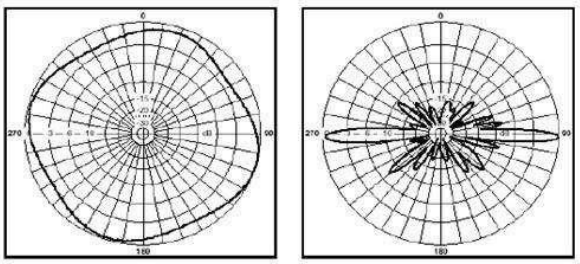
2.7 Antena Omni Directional

Menurut Rachmad Nur (2014) Antena *Omni directional* dalah Antena mempunyai tugas menyelusuri jejak gelombang elektromagnetik, hal ini jika antena berfungsi sebagai penerima. Sedangkan jika sebagai pemancar maka tugas antena tersebut adalah menghasilkan sinyal gelombang elektromagnetik. Antena dapat juga didefinisikan sebagai sebuah atau sekelompok konduktor yang digunakan untuk memancarkan atau meneruskan gelombang elektromagnetik menuju ruang bebas atau menangkap gelombang elektromegnetik dari ruang

Antena omni mempunyai sifat umum radiasi atau pancaran sinyal 360- derajat yang tegak lurus ke atas. *Omni directional* antena secara normal mempunyai gain sekitar 3-12 dBi. Yang digunakan untuk hubungan *Point-To-Multi-Point* (P2Mp) atau satu titik ke banyak titik di sekitar daerah pancaran. Yang baik bekerja dari jarak 1-5 km, akan menguntungkan jika client atau penerima menggunalan directional antenna atau antenna yang terarah. Yang ditunjukkan di bawah adalah pola pancaran khas RFDG 140 omni directional antena. Radiasi yang horisontal dengan pancaran 360-derjat. Radiasi yang horisontal pada dasarnya E-Field (Nurjanah, 2017).



Gambar 2.1 Antenna *Omni Directional*



Gambar 2.2 Pola Radiasi Antenna *Omni*

2.8 *Wireless Card PCI*

Menurut Hasan, Ibrahim (2016) *Wireles card PCI (Peripheral Component Interconnect)* merupakan perangkat *wirelles* berbentuk card PCI yang dipakai dalam sebuah PC yang tidak memiliki perangkat *embedded wireles* di dalamnya. Perangkat ini dapat dipasang pada slot PCI yang terdapat pada komputer. Kebanyakan perangkat ini memiliki jangkauan sinyal yang kecil sehingga kadang pengguna menambahkan perangkat antena tambahan untuk menambah kekuatan tangkap sinyal yang ada

Gambar 2.3 Wireless card PCI-e

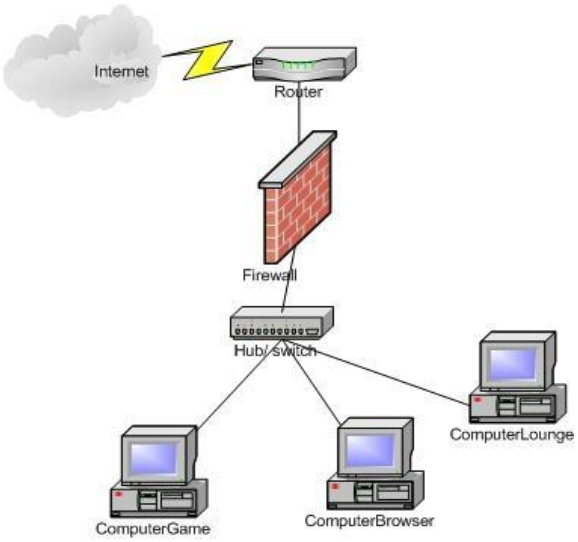
2.9 Kabel *Pigtail*

Menurut Buaton (2012) Kabel *Pigtail* diperuntukkan sebagai penghubung antara antena omni dengan *PCI WLAN* Pada frekuensi 2,4 GHz, biasanya menggunakan konektor tipe N untuk antena maupun kabel coaxial yang \

Gambar 2.4 Kabel *Pigtail*

2.10 Firewall

Menurut Darmadi (2018) *Firewall* merupakan salah satu bagian dari keamanan jaringan (termasuk keamanan internet) yang paling mudah untuk diimplementasikan pada jaringan komputer apapun. Serta mudah untuk konfigurasi secara manual. Pada jaringa LAN, *Firewall* berfungsi untung melindugi setiap komputer *user* dari serangan konten-konten berbahaya yang tidak diinginkan. Dapat juga untuk menjaga keamanan jaringan komputer termasuk-data-data.



2.5 ilustrasi firewall

2.10.1 Fungsi *Firewall*

Menurut Prasetyo Dodi (2014) Sebelum memahami fungsi *firewall* mari kita fahami atribut pentingnya sebagai berikut ;

1. Semua jaringan komunikasi melewati *firewall*
2. Hanya lalu lintas resmi diperbolehkan oleh *firewall*
3. Memiliki kemampuan untuk menahan serangan internet

Fungsi *firewall* sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi *Firewal* mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan *firewall* apakah memperbolehkan paket data lewati atau tidak, antara lain :

1.Alamt IP dari computer sumber

2. Port TCP/UDP sumber dari sumber

3. Alamt IP dari computer tujuan

4. Port TCP/UDP tujuan data pada computer tujua

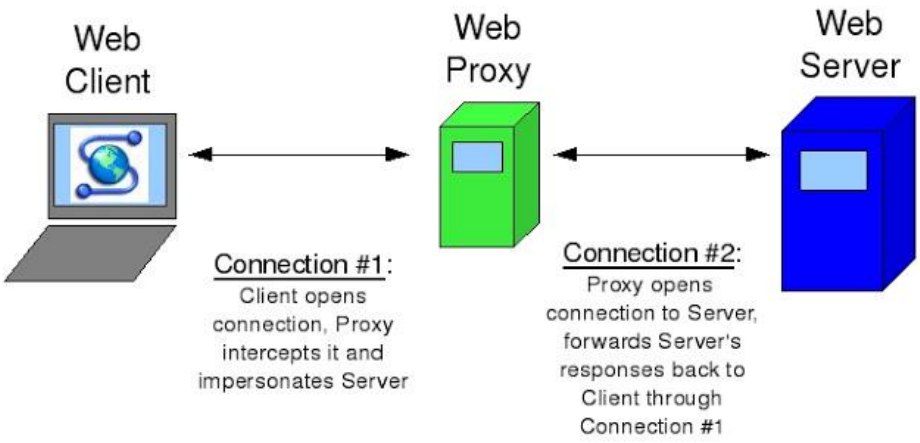
5. Informasi dari header yang disimpan dalam paket data.

Secara spesifik Fungsi *Firewall* adalah melakukan *autentifikasi* terhadap akses kejaringan. Applikasi *proxy Firewall* mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

Fungsi *proxy* dapat dilakukan oleh sebagai *software* , tergantung pada jenis *proxy* yang dibutuhkan pada jenis *proxy* Yang dibutuhkan, misalnya web *proxy*, *login proxy,* ftp *proxy,* dan seterusnya. Di sisi *client* sering kali dibutuhkan *software* tertentu agar dapat menggunakan *proxy* server misalnya dengan menggunakan SOCKS.

2.11 Penjelasan Web Proxy Mikrotik

Menurut Sujalwo (2011) *Proxy* adalah suatu aplikasi yang menjadi perantara antara client dengan *server*, sehingga *client* tidak akan berhubungan langsung dengan *server-server* yang ada di Internet. Mikrotik memiliki fitur *Web proxy* yang bisa digunakan sebagai *proxy server* yang nantinya akan menjadi perantara antara *browser* user dengan *web server* di Internet.



Gambar 2.6 Cara kerja Web Proxy

2.11.1 Cara Kerja Web Proxy

Menurut Kusnawi (2012) Ketika user membuka suatu situs, maka browser akan mengirimkan HTTP *request* ke *Server*, namun karena komputer *user* ini menggunakan *web proxy* maka *proxy* akan menerima HTTP *request* dari *browser* tersebut kemudian membuat HTTP *request* baru atas nama dirinya. HTTP *request* baru buatan *Proxy* inilah yang diterima oleh *Server* kemudian *Server* membalas dengan HTTP *Response* dan diterima oleh *Proxy* yang kemudian diteruskan ke *browser user* yang sebelumnya melakukan *request* (Witantri, 2016).

2.11.2 Perbedaan Web Proxy dengan NAT

Wijayanta, Setya (2013)Mungkin penjelasan cara kerja *web proxy* di atas hamper mirip dengan NAT *(Network Address Translation) Masquerade,* namun sebenarnya berbeda. Karena jika menggunakan NAT, maka *Mikrotik* hanya akan meneruskan HTTP Request yang dibuat oleh computer user. HTTP request tersebut diteruskan ke Server oleh *Mikrotik* tanpa membuat HTTP r*equest* baru seperti halnya pada *Web Proxy.*

NAT hanya menangani paket data saja, sedangkan Proxy bekerja dengan memeriksa konten dari HTTP *Request* dan *Response* secara detail, sehingga *Proxy* sering juga disebut sebagai *Application Firewal*

2.11.3 Web Proxy Membutuhkan Resource CPU Besar

Wijayanta, Setya (2013)Jika mengaktifkan fitur *Web proxy* pada Mikrotik anda harus memperhatikan kapasitas memori dan CPU. Karena Mikrotik akan membuat HTTP *Request* baru atas nama dirinya, sehingga membutuhkan pemakaian *Resource* memori dan CPU yang lebih besar daripada hanya menggunakan NAT. Jika pemakaian *resource Mikrotik* berlebihan maka akan membuat *Router Mikrotik* anda hang dan koneksi internet pun akan jadi lambat (Witantri, 2016).

Keuntungan menggunakan Web Proxy

Fungsi dari *proxy* secara umum adalah sebagai *Caching, Filtering,* dan *Connection Sharing*. Semua fungsi ini dapat anda temui pada *Web Proxy Mikrotik*. Berikut ini adalah Keuntungan / Manfaat *Web Proxy* pada Mikrotik

Caching

Web Proxy Mikrotik dapat melakukan *caching content* yaitu menyimpan beberapa konten *web* yang disimpan di memori Mikrotik. Konten tersebut akan digunakan kembali

apabila ada permintaan pada konten itu lagi. Misalnya anda membuka Facebook.com, maka file-file pada web tersebut seperti *image, script*, dll akan disimpan oleh *web proxy*, sehingga jika lain kali anda membuka Facebook maka tidak perlu konek ke Internet pun halaman itu bisa dibuka dengan mengambil file dari *cache proxy*. Hal ini dapat menghemat *bandwidth* Internet dan mempercepat koneksi.

Filtering

Dengan menggunakan *Web Proxy* anda dapat membatasi akses konten-konten tertentu yang di *request o*leh *client.* Anda dapat membatasi akses ke situs tertentu, ekstensi file tertentu, melakukan *redirect* (pengalihan) ke situs lain, maupun pembatasan terhadap metode akses HTTP. Hal tersebut tidak dapat anda lakukan jika hanya menggunakan NAT.

Connection Sharing

Web Proxy meningkatkan level keamanan dari jaringan anda, karena computer user tidak berhubungan langsung dengan *web server* yang ada di Internet.

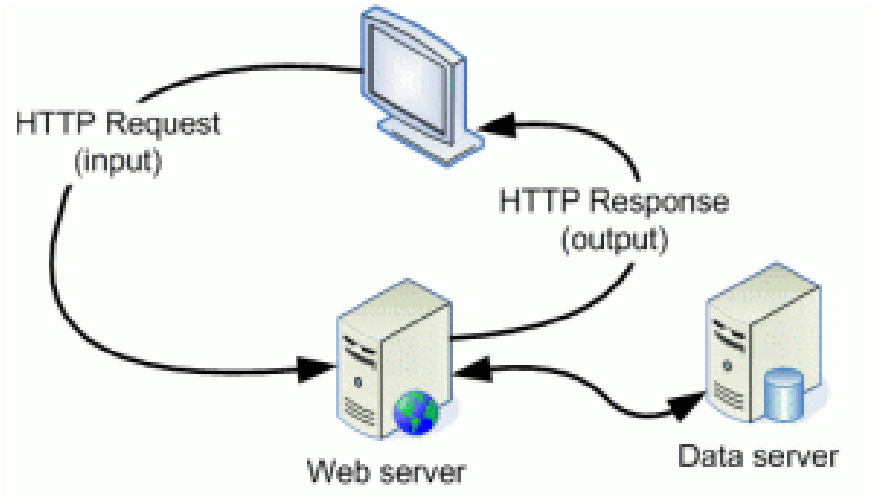
2.11.4 Perbedaan Web Proxy Dan Web Server

Menurut Khasanah Nidaul, Fata (2017) *Web Server* Adalah Sebuah *software* yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS pada klien yang dikenal dan biasanya kita kenal dengan nama *web browser* dan untuk mengirimkan kembali yang hasilnya dalam bentuk beberapa halaman *web* dan pada umumnya akan berbentuk dokumen HTML. itulah pengertian *web server* sebenarnya. dalam bentuk sederhana *web server* akan mengirim data HTML kepada permintaan *web Browser* sehingga akan terlihat seperti pada umumnya yaitu sebuah tampilan *website.*

Web Proxy adalah suatu aplikasi yang menjadi perantara antara *client* dengan *server*, sehingga *client* tidak akan berhubungan langsung dengan *server-server* yang ada di Internet. Mikrotik memiliki fitur *Web proxy* yang bisa digunakan sebagai *proxy server* yang nantinya akan menjadi perantara antara *browser user* dengan *web server* di Internet (Putra Hidayat, 2017).

Cara Kerja Web Server

1. Menerima permintaan *(request)* dari *client,* dan
2. Mengirimkan apa yang diminta oleh *client (response*).



Gambar 2.7 Cara kerja web proxy

Untuk penjelasannya silahkan simak yang berikut ini :

Client disini dapat berupa komputer *desktop* dengan minimal memiliki *browser* dan terhubung ke *web server* melalui jaringan (intranet atau internet).
Komputer yang berfungsi sebagai *server*, dimana didalamnya terdapat perangkat lunak *web server*. Agar komputer ini dapat diakses oleh *client* maka komputer harus terhubung ke jaringan (intranet atau internet). Dalam jaringan internet, komputer ini bisa saja bernama *http://www.google.com*, *http://www.bl.ac.id*, atau memiliki kode komputer (disebut IP Address) seperti 202.10.20.10 dan 200.100.50.25.

Pertama-tama, *client (user)* akan meminta suatu halaman ke *(web) server* untuk ditampilkan di komputer *client.* Misalnya *client* mengetikkan suatu alamat (biasa disebut URL) di *browser http://www.google.com. Client* menekan tombol Enter atau klik tombol *Go* pada *browser*. Lalu apa yang terjadi? Melalui media jaringan (bisa internet, bisa intranet) dan melalui protokol http, akan dicarilah komputer bernama *http://www.google.com*. Jika ditemukan, maka seolah-olah terjadi permintaan, "hai google, ada client yang minta halaman utama nih, ada dimana halamannya?". Inilah yang disebut *request.*

Sekarang dari sisi *server (web server).* Mendapat permintaan halaman utama google dari *client*, si *server* akan mencari-cari di komputernya halaman sesuai permintaan. Namanya juga mencari, kadang ketemu, kadang juga tidak ketemu. Jika ditemukan, maka halaman yang diminta akan dikirimkan ke *client* (si peminta), namun jika tidak ditemukan, maka server akan memberi pesan "404. Page Not Found", yang artinya halaman tidak ditemukan.

Kelebihan proxy server

1. *Open Source*
2. Proses instalasinya mudah
3. Mudah untuk dikustomisasi (Apache hanya punya 4 file konfigurasi) ataupun menambah
4. Peripheral dalam web servernya
5. Bisa digunakan di berbagai platform mesin dari mainframe sampai embedded system
6. Ada komunitas yang besar sehingga mudah mencari solusinya jika ditemukan masalah
7. Mudah dicari di internet.
8. *Server Apache* otomatis berkomunikasi dengan clientnya untuk mendapatkan tampilan *web* terbaik
9. Keamanannya bagus dan bisa menggunakan SSL *(Secure Socket Layer*)

kekurangan

1. Tidak bisa mengatur load seperti IIS sehingga akan terus memfork proses baru sampai dalam batas yang diijinkan OS. Akan memudahkan penyerang karena RAM akan cepat habis
2. Mudah diserang oleh DoS (pada Apache versi 1.3 dan versi 2 sampai versi 2.0.36)
3. Apache tidak memproses karakter kutip dalam string Referrer dan User-Agent yang
4. Dikirimkan oleh Client. Ini berarti Client dapat memformulasi inputnya secara hati-hati untuk
5. Merusak format baris log akses

2.12 Pengertian Jaringan Komputer

Menurut Ikhsan Muhammad (2009) jaringan komputer adalah komunikasi data dari suatu komputer ke komputer yang lain. Untuk pertamakalinya komunikasi data antar komputer tersebut hanyalah bersifat *point-to-point* jadi hanya ada dua komputer yang akan terhubung. Setelah lama berkembang konsep tersebut dikembangkan sehingga pertukaran data yang saat itu bersifat pertukaran antar 2 komputer berubah menjadi jaringan komputer. Konsep jaringan komputer berbeda dengan konsep komunikasi data biasa, dimana beberapa komputer akan saling

terhubung dengan kabel sehingga tiap–tiap komputer dapat saling bertukar data. Pada awalnya implementasi jaringan komputer adalah menggunakan kabel. Seiring dengan perkembangan jaman dan tututan kecepan transmisi data teknologi kabel terus berkembang mulai dari *coaxial* dengan kecepatan 10Mbps, UTP 10BaseT, UTP 100BaseT, coaxial 100Mbps, dan hingga saat artikel ini ditulis telah keluar teknologi UTP dengan kecepatan

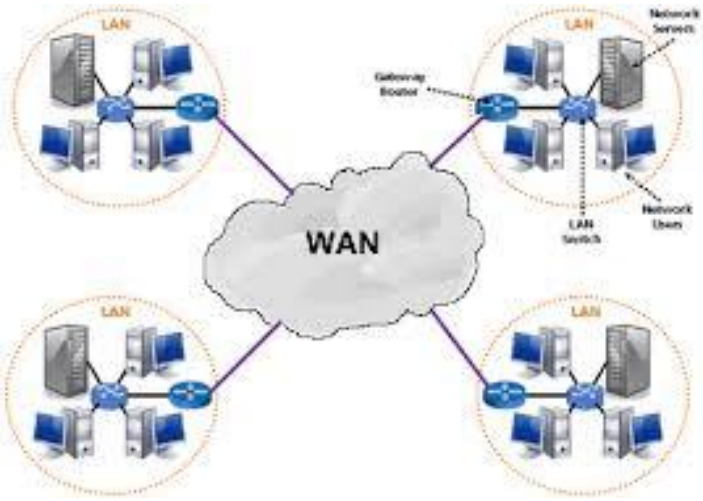
1Gbps. Selain penggunaan kabel dan teknologi semakin berkembang maka keluar transmisi data menggunakan serat optik, dimana kecepatan transfer data jauh melebihi menggunakan kabel. Tetapi semua itu masih belum cukup karena semua teknologi

2.12.1 Tipe-Tipe Jaringan Komputer

1. WAN *(Wide Area Networking)*
2. MAN *(Metropolitan Area Networking)*
3. LAN (*Local Area Networking)*
4. Wireless Fidelity (Wi-fi)

2.12.2 WAN *(Wide Area Networking)*

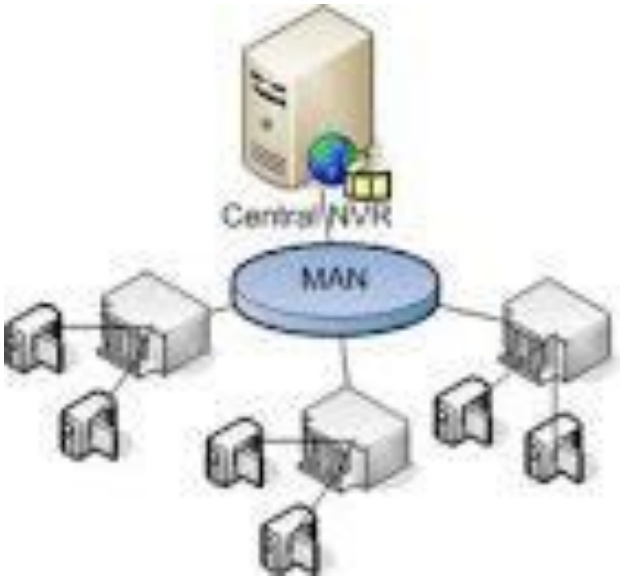
Menurut Ikhsan Muhammad (2009) Wan adalah Jaringan yang merupakan hubungan antara beberapa komputer yang sifatnya beda negara. Contohnya adalah komputer yang berada di Indonesia berhubungan dengan komputer yang ada di Washington DC, US



Gambar 2.8 Topologi WAN

2.12.3 MAN (*Metropolitan Area Networking)*

Menurut Ikhsan Muhammad (2009) MAN adalah jaringan yang merupakan hubungan antara beberapa komputer yang berbeda kota. Contohnya adalah komputer cabang Jakarta berhubungan dengan komputer yang ada di cabang Bandung. Teknis hubungan MAN dilakukan bisa dilakukan dengan cara yang sama seperti pada WAN).



Gambar 2.9 Topologi MAN

2.12.4 LAN *(Local Area Networking)*

Menurut Ikhsan Muhammad (2009) Merupakan hubungan antara beberapa komputer yang letaknya tidak berjauhan dan masih dimiliki oleh satu organisasi/institusi. LAN memiliki 4 model yaitu:

a. P2P (Peer to Peer)
b. Workgroup
c. Domain

Gambar 2.10Topologi LAN

2.13 Karakteristik Firewall

1. *Firewall* harus lebih kuat dan kebal terhadap serangan luar. Hal ini berarti bahwa Sistem Operasi akan relatif lebih aman dan penggunaan sistemnya dapat dipercaya.
2. Hanya aktivitas atau kegiatan yang dikenal/terdaftar saja yang dapat melewati atau melakukan hubungan. Hal ini dilakukan dengan menyetting *policy* pada konfigurasi keamanan lokal.
3. Semua aktivitas atau kegiatan dari dalam ke luar harus melewati *firewall*. Hal ini dilakukan dengan membatasi atau memblok semua akses terhadap jaringan lokal, kecuali jika melewati *firewall* terlebih dahulu.

   Firewall ini berjalan pada satu host atau lebih, dan firewall ini terdiri dari beberapa komponen *software*. *Firewall* sendiri mempunyai empat tipe, yaitu *Screened* Subnet *Firewall, Screened Host Firewall, Dual-homed Gateway Firewall,* dan Packet-*filtering Firewall*. Berikut penjelasannya :
4. *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.
5. *Screened Host Firewall* ini terdiri dari sebuah *bastion host (host* yang berupa *application level gateway*) dan dua *router packet filtering*.
6. *Dual-homed Gateway Firewall* ini sedikitnya memiliki dua IP address dan dua *interface* jaringan dan apabila ada serangan dari luar dan tidak dikenal maka akan diblok.
7. *Packet-filtering Firewall* ini terdiri dari router diantara jaringan internal dan eksternal yang aman. Tipe ini untuk menolak dan mengijinkan trafik

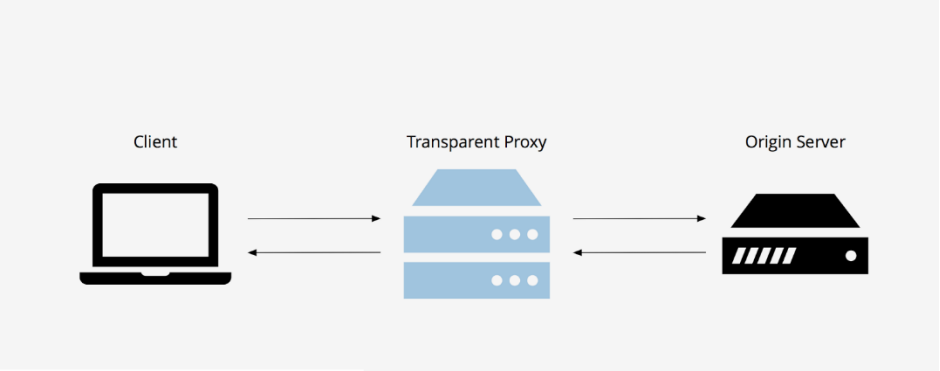
2.14 Jenis Proxy yang diwajibkan diketahui penggunaan proxy

1. Proxy Transparan (Transparent Proxy)

Proxy transparan merupakan salah satu jenis *proxy* yang sebaiknya tidak perlu digunaka. Karena jenis ini adalah *proxy* yang sama sekali tidak merahasiakan alamat IP penggunanya, sehingga alamat IP pengguna akan terlihat jelas oleh publik di dunia maya. Bahkan penggunaan *proxy transparan* juga disebut-sebut bisa membuat alamat IP pengguna diblokir *(banned)* secara permanen dan ini juga membuat pengguna tidak bisa mengakses situs-situs tertentu.

Namun jika *proxy* ini sudah dikonfigurasikan secara khusus untuk penggunaannya, maka pengguna tidak akan mendapati alamat IP diblokir seperti yang sudah disebutkan di atas. *Proxy* transparan sendiri biasanya banyak diaplikasikan pada perusahaan-perusahaan untuk

mengakses informasi lokal. Misalnya seperti informasi seputar perusahaan yang hanya bisa diakses oleh karyawan di sekitaran lokasi perusahaan saja.



Gambar 2.11 Transparant proxy

2. Proxy Anonim (Anonymous Proxy)

Proxy anonim merupakan jenis *proxy* yang tidak membuat alamat IP asli penggunanya terdeteksi, namun hanya akan terlihat alamat IP samaran yang tidak mencurigakan di dunia maya. Adapun ketika pengguna mengakses internet, alamat IP adalah barang wajib yang harus ada agar pengguna tersebut dapat terhubung ke internet. Tanpa alamat IP kemungkinan sangat mustahil bagi pengguna bisa terhubung ke internet.

Untuk hal itulah *proxy* anonim ini digunakan; misalkan ketika pengguna mengakses sebuah *website*, otomatis *website* tersebut akan mengetahui alamat IP yang digunakan oleh pengguna. Namun jika menggunakan *proxy anonim*, *website* tersebut tidak akan mengetahui alamat IP asli milik pengguna tapi yang terdeteksi hanyalah alamat IP *proxy server* saja. Intinya *proxy* ini bisa digunakan untuk menyamarkan alamat IP asli dan bahkan penggunaan *proxy* anonim juga dipercayai meningkatkan keamanan data milik pengguna.

3. High Anonymity Proxy

Proxy yang satu ini tidak mendefinisikan dirinya sebagai sebuah *proxy server*, sehingga tidak menyediakan alamat IP. Dan ketika pengguna mengakses sebuah situs, maka alamat IP pengguna tidak akan terbaca oleh situs bersangkutan maupun internet, namun justru terbaca sebagai sebuah klien. Secara tidak langsung hal ini mengartikan bahwa *high anonymity proxy* sangat merahasiakan alamat IP penggunanya.

4. Distorting Proxy

Distorting proxy fungsinya hampir mirip dengan *anonim proxy*, yakni sama-sama tidak membuat alamat IP asli penggunanya terlihat. Namun perbedaanya terletak pada—jika anonim *proxy* mengubah alamat IP asli penggunanya menjadi alamat IP proxy server, maka *distorting*

proxy ini justru mampu merekayasa alamat IP asli milik pengguna. Sedangkan IP aslinya sendiri hanya dapat dilihat pada HTTP HEADER.

5. Reverse Proxy

Reverse proxy pada dasarnya digunakan untuk menyediakan jalan atas berbagai permintaan pengguna dari internet melalui sebuah *firewall* yang terisolasi atau melalui jaringan pribadi. Adapun untuk fungsinya sendiri, *reverse proxy* biasa digunakan untuk mencegah pengguna terhubung ke internet dengan akses yang tak termonitor. Selain itu, jenis *proxy* ini kerap diaplikasikan pada perusahaan-perusahaan yang membatasi penggunanya untuk membuka situs-situs tertentu, dan biasanya digunakan pada jaringan lokal seperti intranet

Cara kerja *firewall*

Firewall sendiri berada diantara internet dan komputer yang berfungsi sebagai perlindung. *Firewall* menganalisa jaringna yang mencoba masuk ke komputer anda, dan melakukan apa harus dilakukan mengizinkan atau menolak jaringan tersebut.

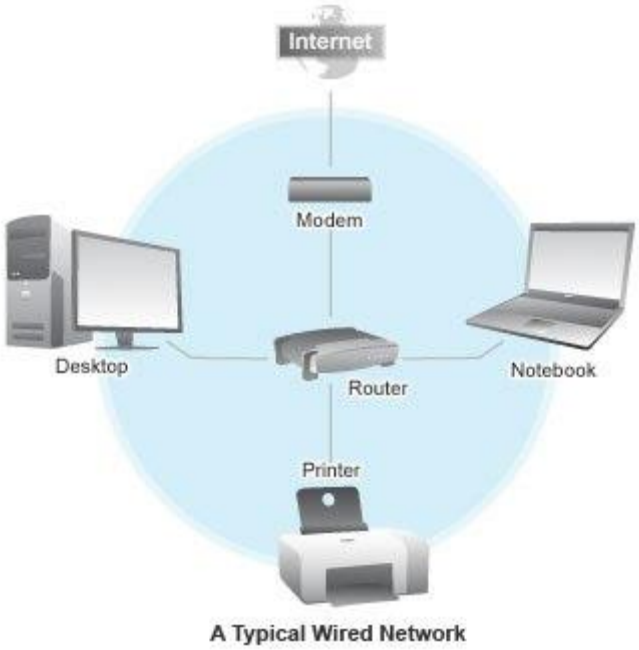
Cara kerja *proxy*

Ketika *user* mengunakan layanan *proxy* lalu melakukan permintaan yang berbeda di internet maka layanan *proxy* harus meneruskan permintaan itu kepada ke internet seakan *proxy* tersebut ituah yang memintanya. Ketika *proxy* telah mendapatkan permintaan *user* tersebut maka *proxy* akan memberikan jawaban kepada *user* dan seakan *proxy* itulah *public* servernya

2.15 Jenis jaringan berdasrkan trasnmiter yang digunakan

2.15.1 Jaringan Kabel *(wired Network)*

Jaringan Berkabel *(wired network)* adalah sebuah jaringan yang berfungsi untuk satu komputer dengan komputer lain, diperlukan penguhubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik atau komputer jaringan



Gambaar 2.12 Jaringan Kabel

Kelebihannya:

1. Relatif murah
2. Tingkat keamanan relatif tinggi
3. Performa / Stabilitas jaringan dan bandwith yang lebih tinggi dan lancar
4. mudah dalam instalasi
5. Biaya yang murah dalam investasi jaringan

Kelemahannya:

1. Kerapian yang kurang(nilai estetika) karena kabel yg berantakan /sembraut
2. Jangkauan dan akses client yang terbatas
3. Susah jika ada perluasan jaringan
4. Wired LAN harus di tempatkan di tempat yang aman
5. *Security* pada wired LAN akan hilang pada saat kabel jaringan di potong

2.16 Jaringan tanpa kabel

Jaringan *nirkabel/wireless* adalah bidang disiplin yang berkaitan dengan komunikasi antar sistem komputer tanpa menggunakan kabel. Jaringan nirkabel ini sering dipakai untuk jaringan komputer baik pada jarak yang dekat (beberapa meter, memakai alat/pemancar bluetooth) maupun pada jarak jauh (lewat satelit). Bidang ini erat hubungannya dengan bidang

telekomunikasi, teknologi informasi, dan teknik komputer. Jenis jaringan yang populer dalam kategori jaringan nirkabel ini meliputi: Jaringan kawasan lokal nirkabel (*wireless* LAN/WLAN), dan Wi-Fi.

Jaringan nirkabel biasanya menghubungkan satu sistem komputer dengan sistem yang lain dengan menggunakan beberapa macam media transmisi tanpa kabel, seperti: gelombang radio, gelombang mikro, maupun cahaya infra merah

Gambar 2.13 Jaringan tanpa kabel

Kelebihannya:

1. Jaringan rapi dan mempunyai nilai estetika,tidak ada kabel yg sembraut
2. Kemudahan proses instalasi
3. Mudah untuk perluasan jaringan
4. Pengurangan anggaran biaya
5. Jangkauan luas
6. Pemeliharaan murah
7. Infrastruktu berdimensi kecil

Kelemahannya:

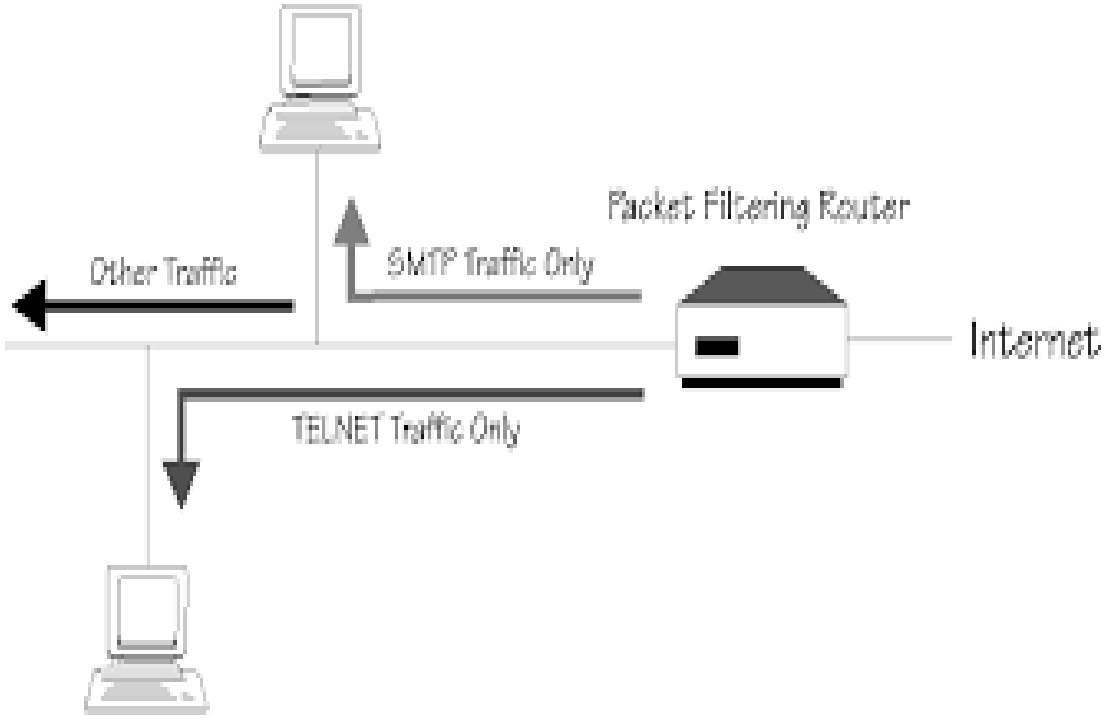
1. Gangguan gelombang jaringan
2. Keamanan data kurangterjamin
3. Konfigurasi yang lebih rumit
4. Tidak stabil dan terpengaruh cuaca

5. Kapasitas jaringan karena keterbatasan spektrum

2.17 Packet Filtering Router

Packet Filtering diaplikasikan dengan cara mengatur semua packet IP baik yang menuju, melewati atau akan dituju oleh packet tersebut.pada tipe ini packet tersebut akan diatur apakah akan di terima dan diteruskan , atau di tolak.penyaringan packet ini di konfigurasikan untuk menyaring packet yang akan di transfer secara dua arah (baik dari atau ke jaringan lokal).

turan penyaringan didasarkan pada header IP dan transport header,termasuk juga alamat awal(IP) dan alamat tujuan (IP),protokol transport yang digunakan(UDP,TCP), serta nomor port yang digunakan. Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, lebih cepat . Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi.



Gambar 2.14 Packet Filtering

2.18 Perbedaan Antara Proxy dan Firewall

Tentang Proxy

Proxy merupakan server yang terdapat di internet dan tujuannya adalah untuk menyediakan suatu layanan agar dapat meneruskan setiap permintaan user kepada server lain. Dengan kata lain proxy berperan sebagai penghubung antara suatu computer dengan internet.

Proxy server bekerja dengan sangat sederhana, yaitu saat user menggunakan layanan proxy dan kemudian user meminta file atau data yang terdapat di public server (internet) maka

proxy akan meneruskannya ke internet, sehingga seolah-olah proxy tersebut yang memintanya. kemudian ketika proxy server telah mendapatkan apa yang telah diminta oleh user, proxy akan memberikan respon kepada user sehingga seolah-olah dialah public servernya

Cara kerja Proxy server

Sebenarnya prinsip kerja proxy server ini sangatlah sederhana, yakni pada user menggunakan layanan suatu proxy kemudian meminta file atau juga data yang terdapat di public server (internet) maka proxy ini akan meneruskannya ke internet jadi seolah-olah proxy ini yang memintanya. Dan pada saat proxy server sudah mendapatkan apa yang diminta oleh user, proxy ini akan memberikan respon kepada user jadi seolah-olah dialah yang merupakan public servernya.

2.19 Kegunaan Proxy

Web proxy merupakan komputer server yang bertindak yakni sebagai komputer lainnya berfungsi untuk dapat melakukan request terhadap kontent dari suatu jaringan internet maupun juga jaringan intranet. Adapun hal-hal yang dapat dilakukan oleh web proxy diantaranya yakni sebagai berikut ini

1. Dapat menyembunyikan alamat IP address.
2. Dapat juga dipakai untuk dapat mengakses suatu website yang sudah di blok oleh ISP (Internet service provider) atau juga oleh suatu organisasi.
3. Dapat juga di gunakan untuk men-blok beberapa atau juga sebuah website yang nantinya akan tidak dapat diakses.
4. Dapat men-filter cookies yang tidak di inginkan serta juga seluruh cookies yang tersimpan di encrypt.
5. Dan juga dapat meningkatkan keamanan privacy pengguna.

2.20 Fungsi Web Proxy

1. Fungsi conecting sharing

Salah satu fungsi proxy ialah sebagai connecting sharing yakni sebagai penghubung atau juga sebagai perantara pengambilan data dari suatu alamat IP serta diantarkan ke alamat IP lainnya ataupun kepada IP komputer user

2. Fungsi filtering

Terdapat beberapa proxy yang dilengkapi dengan firewall yang bisa memblokir beberapa atau juga sebuah alamat IP yang tidak diinginkan, sehingga beberapa dari website tidak dapat diakses dengan memakai proxy tersebut. Itulah salah satu fungsi dari proxy yakni sebagai filtering.

3. Fungsi caching

Kemudian fungsi dari proxy yang lainnya ialah sebagai fungsi caching, maksudnya ialah proxy ini juga dilengkapi dengan media penyimpanan data dari suatu web, dari query ataupun juga permintaan akses user. Contohnya permintaan untuk mengakses suatu web dapat lebih cepat apabila sudah ada permintaan akses ke suatu web pada pemakai proxy sebelumnya. Itulah fungsi dari proxy yakni sebagai chacing