**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan, maka pihak pengelolah jaringan komputer mengalami kendala dalam pengelolaan lalulintas data. Karena kurangnya pengelolaan lalulintas data dalam jaringan komputer, maka terjadi penurunan performa seperti berkurangnya kecepatan pengiriman data, dikarenakan pengguna memiliki hak akses jaringan yang hampir tidak terbatas. Tentunya masalah performa merupakan hal yang kritis dalam jaringan komputer.

Access Control List (ACL) merupakan salah satu alternatif untuk pengelolaan lalulintas data serta hak akses dari masing-masing pengguna. ACL adalah suatu rentetan listdari suatu statemen perijinan atau penolakan yang di tujukan ke alamat – alamat dalam jaringan komputer. ACL umumnya dijalankan pada perangkat jaringan Router. Router sendiri merupakan salah satu intermediary device (alat perantara) yang berfungsi sebagai penghubung dua atau lebih jaringan komputer agar dapat saling berkomunikasi.

Dengan menerapkan ACL, maka dapat dilakukan pembatasan pada jaringan komputer. Proses yang terjadi dalam jaringan komputer hanyalah komunikasi antara sesama komputer, komputer dengan perangkat perantara jaringan, ataupun perangkat perantara jaringan dengan perangkat perantara jaringan lainnya. Pembatasan yang dilakukan dalam proses komunikasi di dalam jaringan komputer mencakup pembatasan pengiriman data dan pembatasan hak akses dari pengguna dalam jaringan komputer. Namun dalam implementasinya, penulis menemui ada beberapa kekurangan yang dimiliki oleh ACL. Berdasarkan pada penelitian sebelumnya, tentang ”Monitoring Aktifitas Jaringan Dan Simulasi Access Control List Pada STMIK Palcomtech Berbasis Cisco Router”, oleh Septian Krisna Dinata pada tahun 2013, penulis mendapati adanya pembatasan yang belum dilakukan. Dalam penelitian tersebut hanya dilakukan pembatasan akses website langsung dari sisi pengguna ke alamat tujuan, tidak dilakukan pembatasan yang dapat mebatasi akses dari pengguna melalui sebuah perantara, dalam hal ini sebuah web proxy. Dalam penelitian ini, penulis akan mengimplementasikan proxy server untuk membantu Router dalam melengkapi beberapa kekurangan dari ACL. Proxy server adalah suatu sistem komputer atau aplikasi yang berperan sebagai perantara yang menerima permintaan dari pengguna jaringan ke berbagai sumber di dalam atau luar jaringan komputer.

Berdasarkan alasan dan uraian diatas, maka dibuat suatu penelitian dengan judul : “***Implementasi Proxy Server Untuk Meningkatkan Kemampuan Filter Access Control List Pada Router****”.*

* 1. **Rumusan Masalah**

Berdasarkan latar belakang yang telah diuraikan, terdapat beberapa permasalahan yang dapat dirumuskan sebagai berikut :

1. Bagaimana cara implementasi Proxy Server agar dapat membantu Router dalam melakukan filter akses ?
2. Apa saja kemampuan filter Access Control List yang dapat ditingkatkan pada Router dengan menggunakan Proxy Server?
   1. **Batasan Masalah**

Terdapat beberapa batasan masalah yang diangkat sebagai parameter pengerjaan penelitian ini diantaranya adalah sebagai berikut :

1. Menggunakan Debian 8 sebagai Sistem Operasi Proxy Server.
2. Menggunakan Squid sebagai daemon/layanan untuk menjalankan Proxy Server.
3. Diterapkan pada jaringan Local Area Network (LAN).
4. Menggunakan Router Cisco sebagai acuan peningkatan kemampuan filter Access Control List.
5. Pembatasan hak akses hanya diterapkan pada protokol HTTP atau pada port 80.  
   1. **Tujuan Penelitian**

Dalam penelitian ini terdapat beberapa tujuan diantaranya adalah sebagai berikut :

1. Dapat mengimplementasikan Proxy Server untuk membantu Router dalam melakukan filter akses.
2. Dapat meningkatkan kemampuan filter Access Control List pada Router dengan menggunakan Proxy Server.
   1. **Manfaat Penelitian**

Manfaat yang diperoleh dari penelitian ini adalah dapat memberikan solusi bagaimana cara meningkatkan kemampuan filter Access Control List pada Router.

* 1. **Sistematika Penulisan**

Dalam laporan tugas akhir ini, pembahasan akan disajikan dalam beberapa bab dengan sistematika penulisannya adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan yang digunakan dalam laporan tugas akhir ini.

BAB II TINJ AUAN PUSTAKA

Pada bab ini berisi tentang teori-teori dan penjelasan yang berkaitan dengan permasalahan dan penyelesaian masalah dari laporan tugas akhir.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang analisis, perancangan, dan konfigurasi Router dan Proxy Server dengan menggunakan Squid pada jaringan komputer.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang implementasi konfigurasi Router dan Proxy Server dengan menggunakan Squid pada jaringan komputer. Serta hasil uji coba konfigurasi Router dan Proxy Server dengan menggunakan Squid pada jaringan komputer.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan yang dapat diambil dari keseluruhan isi laporan tugas akhir, dan saran yang diharapkan dapat bermanfaat untuk pengembangan selanjutnya.

DAFTAR PUSTAKA

Pada bagian ini dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembutan laporan tugas akhir ini.

**BAB II**

**TINJAUAN PUSTAKA**

* 1. **Access Control List (ACL)**

Access control list mungkin digambarkan hanya untuk keamanan, meskipun access control list memang digunakan untuk fungsi keamanan. Access control list dipahami sebagai mekanisme umum yang digunakan oleh router cisco untuk menentukan satu set objek jaringan tunduk pada kebijakan yang telah dibuat.

Access control list digunakan untuk mengijinkan atau tidak paket dari user menuju tujuan tertentu atau sebaliknya. Aturan/kebijakan yang telah dibuat kemudian diterapkan ke interface router yang dikehendaki, entah itu interface yang mengarah keluar jaringan maupun ke dalam jaringan.

Terdapat 2 jenis access control list, yaitu:

* Standart ACL

Digunakan untuk memfilter paket hanya berdasarkan source IP address dan diterapkan pada interface yang terdekat dengan source IP address. Standart ACL didefinisikan dengan nomor antara 1 sampai 99.

* Extended ACL

Digunakan untuk memfilter paket berdasarkan source maupun destination IP address, jenis paket, maupun alamat port. Extended ACL didefiniskan dengan nomor antara 100 sampai 199. (*Jeff Sedayao, 2011*)

* 1. **Jaringan Komputer**

Jaringan komputer dapat diartikan sebagai himpunan atau kumpulan komputer – komputer (umunya PC desktop) yang saling terhubung melalui media penghubung (kabel ataupun gelombang radio ataupun medium lain seperti serat optik) untuk melakukan pertukaran data demi tercapainya tujuan tertentu. (*Siti Munawaroh, 2007*) .

Tiap komputer, printer atau periferal yang terhubung dengan jaringan disebut *node*. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan *node*.

Sebuah jaringan biasanya terdiri dari 2 atau lebih komputer yang saling berhubungan diantara satu dengan yang lain, dan saling berbagi sumber daya misalnya CDROM, Printer, pertukaran file, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung tersebut, dimungkinkan berhubungan dengan media kabel, saluran telepon, gelombang radio, satelit, atau sinar infra merah.

Jaringan komputer dapat dibuat berdasarkan kebutuhan, yaitu dengan pilihan bentuk dan ukuran yang beraneka ragam. Pesatnya industri jaringan komputer membuat para praktisi dan para ahli menemukan beragam tipe dan desain jaringan yang dikenal dengan istilah *networking terminology*. Saat ini, terdapat sebelas jenis jaringan komputer, yaitu LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network), SAN (Storage Area Network), System Area Network, Server Area Network, Small Area Network, Personal Area Network, Desk Area Network, Controller Area Network, Cluster Area Network. Pada Laporan ini, hanya dibahas jenis jaringan komputer LAN (Local Area Network).

* 1. **Protokol Jaringan**

**Protokol pada dasarnya adalah sebuah persetujuan semua pihak yang berkomunikasi tentang bagaimana komunikasi tersebut harus dilakukan. Sebuah arsitektur harus terdiri dari informasi yang cukup untuk memungkinkan satu implementasi menulis suatu program atau membentuk perangkat keras bagi setiap layernya. Sehingga cara itu dapat mentaati sepenuhnya protokol yang cocok. Jumlah, nama, isi, dan fungsi setiap layer berbeda dari jaringan yang satu dengan jaringan yang lainnya.**

Jika suatu protokol menerima data sari protokol lain pada layer atasnya, ia akan menambahkan informasi tambahan miliknya ke data tersebut. Informasi ini memiliki fungsi yang sesuai dengan fungsi protokol tersebut. Setelah itu, data ini diteruskan lagi ke protokol pada layer di bawahnya. **(*Siti Munawaroh, 2007*)**

* 1. **Linux Debian**

Debian adalah [sistem operasi](https://id.wikipedia.org/wiki/Sistem_operasi) komputer yang tersusun dari paket-paket perangkat lunak yang dirilis sebagai perangkat lunak bebas dan terbuka dengan lisensi mayoritas *GNU General Public License* dan lisensi perangkat lunak bebas lainnya. Debian GNU/Linux memuat perkakas sistem operasi GNU dan [kernel Linux](https://id.wikipedia.org/wiki/Kernel_Linux) merupakan distribusi Linux yang populer dan berpengaruh.

Debian didistribusikan dengan akses ke repositori dengan ribuan paket perangkat lunak yang siap untuk instalasi dan digunakan. Debian terkenal dengan sikap tegas pada filosofi dari Unix dan perangkat lunak bebas. Debian dapat digunakan pada beragam perangkat keras, mulai dari komputer jinjing dan *desktop* hingga telepon dan server. Debian fokus pada kestabilan dan keamanan.

* 1. **Proxy Server**

Proxy dalam pengertiannya sebagai perantara, bekerja dalam berbagai jenis protokol komunikasi jaringan dan dapat berada pada level-level yang berbeda pada hirarki layer protokol komunikasi jaringan. Suatu perantara dapat saja bekerja pada layer Data-Link, layer Network dan Transport, maupun layer Aplikasi dalam hirarki layer komunikasi jaringan menurut OSI. Namun pengertian Proxy Server sebagian besar adalah untuk menunjuk suatu server yang bekerja sebagai Proxy pada layer Aplikasi. (*Denis Tri Priyono, dkk, 2012*)

*Proxy server* dapat berupa suatu sistem komputer ataupun sebuah aplikasi yang bertugas menjadi *gateway* atau pintu masuk yang menghubungan komputer kita dengan jaringan luar.

Secara umum manfaat *proxy* *server* ada dua macam, yaitu sebagai berikut:

1. Meningkatkan kinerja jaringan**.** Dengan kemampuan *server* *proxy* untuk menyimpan data permintaan dari aplikasi *client*, permintaan yang sama dengan permintaan sebelumnya hanya akan diambilkan dari simpanan *server* *proxy*. Jika seorang pengguna internet sudah pernah membuka situs yang sama, tidak perlu dihubungkan langsung pada situs sumbernya, tetapi cukup diambilkan dari simpanan *server* *proxy*. Dengan cara demikian, koneksi langsung pada *server* sumbernya dapat dikurangi. Dengan demikian, penggunaan *bandwidth* internet untuk koneksi langsung menjadi berkurang.
2. Filter permintaan**.** *Server* *proxy* juga dapat digunakan sebagai filter terhadap permintaan data dari suatu situs. Dalam hal ini, *server* *proxy* menjadi filter terhadap situs yang boleh atau tidak boleh dikunjungi. Selain itu, *server* *proxy* juga dapat sebagai filter terhadap aplikasi *client* yang dapat menggunakan akses terhadap internet. Dalam hal ini *server* *proxy* berlaku sebagai filter terhadap gangguan internet.

Secara prinsip pihak pertama dan pihak kedua tidak langsung berhubungan, akan tetapi masing-masing berhubungan degan pihak ketiga yaitu *proxy*.

Tiga fungsi utama *proxy*:

1. *Connection sharing*

Bertindak sebagai *gateway* yang menjadi batas antara jaringan lokal dan jaringan luar. *Gateway* juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya dan koneksi jaringan luar juga terhubung kepadanya. Dengan demikian koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh *gateway* secara bersama-sama *(connecion sharing)*.

1. *Filtering*

Bekerja pada layar aplikasi sehingga berfungsi sebagai *Firewalll* paket *filtering* yang digunakan untuk melindungi jaringan lokal terhadap gangguan atau serangan dari jaringan luar. Dapat dikonfigurasi untuk menolak situs *web* tertenu pada waktu-waktu tertentu.

1. *Caching*

*Proxy* *Server* memiliki mekanisme penyimpanan obyek-obyek yang sudah diminta dari *server*-*server* di internet. Mekanisme *caching* akan menyimpan obyek-obyek yang merupakan permintaan dari para pengguna yang di dapat dari iternet.

* 1. **IPTABLES**

Iptables adalah suatu tools dalam sistem operasi Linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalulintas data. Secara sederhana digambarkan sebagai pengatur lalulintas data. Dengan iptables inilah kita akan mengatur semua lalulintas dalam server kita, baik yang masuk ke server, keluar dari server, ataupun traffic yang sekedar melewati server kita. Intinya adalah sebuah filtering pada lalulintas network. IP Tables melakukan Pemfilteran berdasar IP - Port atau MAC Adresss. Dalam melakukan Pemfilteran maka IP Tables juga mempunyai sebuah Aturan / privasi policy.

* 1. **Topologi Jaringan**

Topologi jaringan adalah tata cara penghubungan antara satu komputer dengan komputer yang lainnya ke dalam sebuah jaringan. Setiap [jenis topologi jaringan komputer](http://www.adalahcara.com/2014/09/macam-pengertian-topologi-jaringan-komputer.html) akan berbeda dari segi kecepatan pengiriman data, biaya pembuatan, serta kemudahan dalam proses maintenance nya. Dan juga setiap jenis topologi jaringan komputer memiliki kelebihan serta kekurangannya masing-masing. (*Siti Munawaroh, 2007*)

Jenis – jenis topologi jaringan adalah sebagai berikut :

* Topologi Ring
* Topologi Star
* Topologi Bus
* Topologi Tree
* Topologi Mesh
* Topologi Loop Network
  1. **IP Address**

*IP address* adalah alamat logika yang diberikan pada sebuah perangkat jaringan. IP address yang digunakan dalam suatu komputer harus unik dan tidak boleh sama dengan yang lain. IP address terdiri dari deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan komputer. (*Simamora, dkk, 2011*)

Di dalam jaringan, pengiriman suatu paket data membutuhkan alamat sebagai identitas tujuan suatu data akan dikirim (*Destination Address*) dan asal paket (*Source Address*). Namun untuk mengirimkan paket data ke sistem yang berbeda, dibutuhkan sistem pengalamatan yang bersifat universal dan dapat dikenali oleh masing – masing sistem. *IP Address* ditetapkan sebagai sistem pengalamatan yang universal karena memiliki karakteristik yang lebih baik dibanding sistem pengalamatan yang lain.

* 1. **Router**

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya.

* 1. **Switch**

Pengalih jaringan (atau *switch*) adalah sebuah alat jaringan yang melakukan penjembatan taktampak (penghubung penyekatan (*segmentation*) banyak jaringan dengan pengalihan berdasarkan [alamat MAC](https://id.wikipedia.org/wiki/Alamat_MAC)). Switch jaringan dapat digunakan sebagai penghubung [komputer](https://id.wikipedia.org/wiki/Komputer) atau [penghala](https://id.wikipedia.org/wiki/Penghala) pada satu area yang terbatas, pengalih juga bekerja pada lapisan taut data (*data link*), cara kerja pengalih hampir sama seperti jembatan (*bridge*), tetapi switch memiliki sejumlah porta sehingga sering dinamakan jembatan pancaporta (*multi-port bridge*).

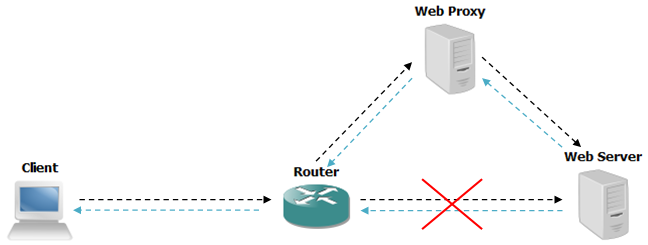
* 1. **Web Cache Communication Protocol**

Web Cache Communication Protocol (WCCP) adalah protokol yang dikembangkan oleh Cisco yang memungkinkan pengalihan transparan lalu lintas jaringan secara real-time. Pengalihan ini bisa untuk mesin cache atau untuk proxy, seperti Web Gateway. Cisco IOS Rilis 12.1 dan seterusnya memungkinkan penggunaan baik Versi 1 (WCCP v1) atau Versi 2 (WCCPv2).

Terdapat 2 versi protokol WCCP, yakni :

* + 1. WCCP Versi 1. Pada versi ini, protokol WCCP hanya mendukung 1 router sebagai WCCP Server, 1 port yang bisa dialihkan yaitu port 80 (HTTP), menggunakan metode enkapsulasi GRE (Generic Routing Encapsulation) dalam pencegahan modifikasi paket data, serta router dan proxy server berkomunikasi melalui port UDP 2048.
    2. WCCP Versi 2. Pada versi ini, protocol WCCP mengalami peningkatan yang signifikan, diantaranya mendukung hingga 32 router sebagai WCCP Server dan 32 Proxy Server sebagai WCCP Client, mendukung semua port TCP dan UDP, dan mendukung hingga 255 service group.
  1. **Web Proxy**

Web Proxy merupakan web berbasis proxy server yang berfungsi sebagai anonymizer. Maksudnya, Web Proxy bertugas sebagai perantara antara anda (client) dengan web server (web tujuan), dan setiap interaksi akan melalui web proxy. Dalam proses pengiriman data, IP Address anda tidak akan nampak pada web server karena web proxy menyembunyikan IP anda secara anonymous.

****

**Gambar 2.1** Model Koneksi Web Proxy

Ketika user membuka suatu situs, maka browser akan mengirimkan HTTP request ke Server, namun karena computer 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

* 1. **URL (Unifrom Resource Locator)**

*Uniform Resources Locator* (URL) adalah sebuah rangkaian karakter yang membentuk suatu “*pathname*” untuk mengidentifikasikan sebuah dokumen atau gambar dalam sebuah *web*.

URL terdiri dari beberapa bagian, seperti:

1. Bagian pertama URL dikenal sebagai protokol atau disebut pula http:// yang merupakan singkatan dari *Hyper-text Transfer Protocol*.
2. Bagian kedua dari URL dikenal sebagai nama domain, domain mewakili nama *server* yang sedang berhubungan dengan internet.
3. Bagian ketiga dari URL disebut dengan *directory path* yang merupakan area khusus dimana domain – domain berada,
4. Bagian keempat dari URL disebut nama *file*, yakni menentukan *file* khusus yang sedang diakses yang biasanya adalah sebuah *file* HTML, gambar, suara dan sebagainya. (*Simamora, dkk, 2011*)

Fungsi URL :

1. Sebagai pengidentifikasi sebuah dokumen di web.
2. Pemberian alamat pada setiap web yang berisi dokumen.
3. Untuk memudahkan kita dalam mengakses suatu dokumen melalui website.
4. Untuk memberikan penamaan terhadap suatu file/dokumen pada website.
5. Memudahkan kita untuk mengingat suatu alamat website.
   1. **Internet**

Definisi internet adalah sebuah jaringan komputer yang terdiri dari berbagai macam ukuran jaringan komputer diseluruh dunia mulai dari sebuah PC , jaringan berskala kecil sampai pada jaringan yang berukuran besar menjadi tulang punggung internet (backbone). Semula internet hanyalah sebuah jaringan kecil yang dibuat untuk Departemen Pertahanan Amerika Serikat yang disebut *Arpanet*. Tetapi kemudian untuk alasan riset maka jaringan itu diperluas dengan dihubungkan dengan jaringan – jaringan perguruan tinggi yang ada. Lama kelamaan jaringan tersebut terus membesar sehingga sampai sekarang ini . Kemudian untuk menangani semua hal – hal yang berkaitan dengan internet maka

didirikanlah badan – badan khusus yang menanganinya.

Nama awal dari jaringan raksasa ini adalah *DARPA Internet*, yang kemudian disingkat hanya menjadi Internet saja. Internet juga dikenal sebagai jaringan informasi dunia ada dan dapat dicari disini .

Komponen – komponen Internet adalah :

* 1. World Wide Web (www)

Bagian dari internet itu sendiri. Web terdiri dari kumpulan besar dokumen – dokumen yang disimpan pada komputer – komputer diseluruh dunia

* 1. Web page

Dokumen elektronik yang terletak di jaringan internet. Web server Komputer yang menyimpan web page – web page dan membuat web page tersebut dapat dilihat orang lain.

* 1. Web site

Koleksi dari web page – web page yang saling berhubungan dan dapat diakses secara elektronik. Web page biasanya dimiliki oleh universitas, pemerintah, perusahaan untuk dapat dilihat oleh banyak orang dari berbagai penjuru dunia. Secara fisik sebuah web site terletak di sebuah web server.

* 1. **NAT (Network Address Translation)**

Fungsi utama dari NAT adalah sebagai sharing Internet apabila pada suatu jaringan hanya memiliki satu IP Public yang dapat dikenali di Internet. Jadi NAT merupakan salah satu cara lain untuk sharing Internet selain mengunakan proxy.(Andreas Handojo, dkk, 2002)

Tipe – tipe NAT :

1. NAT Tipe Statis

NAT Statis menggunakan *table routing* yang tetap, atau alokasi translasi alamat ip ditetapkan sesuai dengan alamat asal atau source ke alamat tujuan atau destination, sehingga tidak memungkinkan terjadinya pertukaran data dalam suatu alamat ip bila translasi alamat IPnya belum didaftarkan dalam *table NAT*. NAT Statia terjadi ketika sebuah alamat lokal*(inside)* di petakan ke sebuah alamat global/internet *(outside)*. Alamat lokal dan global dipetakan satu lawan satu secara statik. NAT secara statis akan melakukan *request* atau pengambilan dan pengiriman paket data sesuai dengan aturan yang telah ditabelkan dalam sebuah NAT.

1. NAT Tipe Dinamis

NAT dengan tipe dinamis menggunakan logika *balancing* atau menggunakan logika pengaturan beban, di mana dalam tabelnya sendiri telah ditanamkan logika kemungkinan dan pemecahannya, NAT dengan tipe dinamis pada umumnya dibagi menjadi 2 jenis yaitu NAT sistem pool dan NAT sistem overload.

1. NAT Sistem Pool

NAT dengan sistem pool atau kelompok menggunakan sebuah tabel NAT dengan logika dinamis, dimana logika yang ditanamkan dalam NAT tersebut pada umumnya merupakan logika *Fuzzy* atau jika lambang yang nilai translasinya belum pasti, dalam sistem pool suatu*request* belum tentu akan melewati jaringan yang sama bila melakukan request yang sama untuk kedua kalinya, Translasi Dinamik terjadi ketika router NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (pool) alamat global yang akan digunakan untuk terhubung ke internet. NAT dengan sistem pool biasanya sering dimanfaatkan untuk melakukan *balancing* atau penyeimbangan beban pada jaringan.

1. NAT Sistem Overload

NAT dengan sistem *Overloading* menggunakan logika *request* atau permintaan dari banyak*client* atau banyak alamat dioperkan atau diberikan ke satu alamat IP distribusi. Sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global *(outside)*. Sejumlah IP Lokal /internal dapat ditranslasikan ke satu alamat IP global (*outside)*. Hal ini sangat menghemat penggunakan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menggunakan metoda *port multiplexing*, atau perubahan *port* ke *packet outbound*.

* 1. **Wildcard**

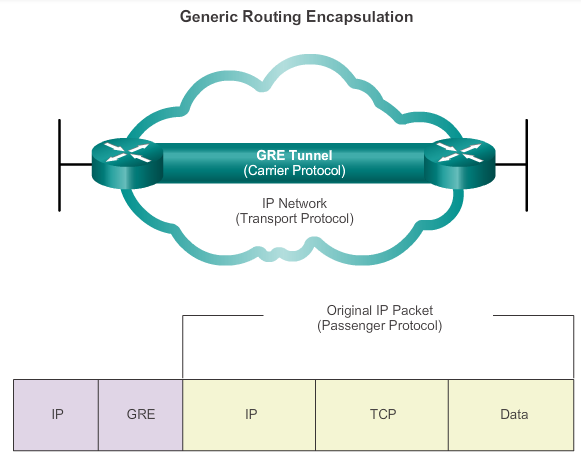
Wildcard Mask adalah suatu urutan angka-angka yang mengefektifkan paket Routing didalam subnets suatu jaringan property. Wildcard mask panjangnya 32-bit yang dibagi menjadi empat octet. Wildcard mask adalah pasangan IP address. Angka 1 dan 0 pada mask digunakan untuk mengidentifikasikan bit-bit IP address. Wildcard mask mewakili proses yang cocok dengan ACL mask-bit. Wildcard mask tidak ada hubungannya dengan subnet mask.Wildcard mask dan subnet mask dibedakan oleh dua hal. Subnet mask menggunakan biner 1 dan 0 untuk mengidentifikasi jaringan, subnet dan host. Wildcard mask menggunakan biner 1 atau 0 untuk memfilter IP address individual atau grup untuk diijinkan atau ditolak akses. Persamaannya hanya satu dua-duanya sama-sama 32-bit.

* 1. **GRE (Generic Routing Encapsulation)**

Generic Routing Encapsulation (GRE) adalah salah satu contoh dari dasar, non-aman, VPN protokol tunneling situs-situs. GRE adalah protokol tunneling yang dikembangkan oleh Cisco yang dapat merangkum berbagai jenis protokol paket di dalam terowongan IP. GRE menciptakan link virtual point-to-point untuk router Cisco pada titik-titik jarak jauh, melalui sebuah internetwork IP. GRE dirancang untuk mengelola transportasi multiprotocol dan lalu lintas IP multicast antara dua atau lebih situs, yang mungkin hanya memiliki konektivitas IP. Hal ini dapat merangkum beberapa jenis protokol paket di dalam sebuah terowongan IP.

Karakteristik GRE :

* GRE didefinisikan sebagai standar IETF (RFC 2784).
* Dalam header IP luar, 47 digunakan dalam bidang protokol untuk menunjukkan bahwa header GRE akan mengikuti.
* GRE enkapsulasi menggunakan lapangan jenis protokol pada header GRE untuk mendukung enkapsulasi dari setiap OSI Layer 3 protokol. Jenis protokol didefinisikan dalam RFC 1700 sebagai “EtherTypes”.
* GRE sendiri adalah stateless; secara default tidak menyertakan mekanisme flow-control.
* GRE tidak termasuk mekanisme keamanan yang kuat untuk melindungi muatannya.
* GRE header, bersama-sama dengan header tunneling IP ditunjukkan pada gambar, menciptakan setidaknya 24 byte overhead tambahan untuk paket terowongan.



(Sumber : [*http://blog.umy.ac.id*](http://blog.umy.ac.id))

**Gambar 2.2** Paket Data GRE

* 1. **Tunneling**

Tunneling mennyediakan suatu koneksi point-to-point logis sepanjang jaringan iP yang bersifat connectionless. Proses transfer data dari satu jaringan ke jaringan lain memanfaatkan koneksi jaringan secara terselubung (tunneling). Ketika paket berjalan menuju ke node tujuan, paket ini melalui suatu jalur yang disebut tunnel.

Disebut tunnel atau salurang karena aplikasi yang memanfaatkannya hanya melihat dia end point, sehingga paket yang lewat pada tunnel hanya akan melakukan satu kali lompatan atau hop. Koneksi tunnel juga memungkinkan dilakukannya koneksi secara pribadi antar user sehingga keamanan paket data lebih terjamin dibandingkan menggunakan model koneksi pada umumnya.