PERANCANGAN SISTEM KONEKTIFITAS INTRANET-INTERNET DENGAN MENGGUNAKAN KONSEP NAT

A.W. Purwandi *)

ABSTRACT

Intranet can be related to the Internet, and vice versa. To connect your intranet to the internet a lot of things to watch for the efficient and effective connectivity. Some important things that are addressing and internet security. Internet protocol used in the TCP / IP (Transmission Control Protocol / Internet Protocol), requires that every host or intend to connect computers into a network must have a unique IP address. So that when the intranet was about to be connected to the internet or any host computer that is connected must have an IP address in accordance with the rules of the addressing used in the internet. The concept of NAT (Network Address Translator) provides a solution to overcome the limitations of available IP addresses. Masquereding IP is the internet service which is the application of the concept of NAT that can reduce the demand for new IP addresses connecting ourselves into the internet and intranet can improve security. Masquereding IP is one of the additional capabilities on LINUX operating system.

***Keywords**: TCP / IP, NAT Concepts, IP Masquerading, LINUX.*

PENDAHULUAN

1. Latar Belakang

Teknologi Internet berkembang dengan pesat sehingga menjadi salah satu media yang efektif dan efisien dalam memperoleh dan menyebarkan informasi. Perkembangan teknologi internet ini telah membuat landasan teknologi baru untuk diterapkan pada lingkungan yang lebih kecil seperti perusahaan atau organisasi yang dikenal sebagai intranet.

Intranet dapat berhubungan dengan internet, begitu pula sebaliknya. Untuk mengkoneksikan intranet dengan internet banyak hal yang harus diperhatikan agar konektifitas tersebut efisien dan efektif. Beberapa hal penting itu adalah pengalamatan dan keamanan internet.

Protokol yang digunakan dalam internet yaitu TCP/IP (*Transmission Control Protocol / Internet Protocol*), mengharuskan setiap host atau komputer yang hendak dihubungkan kedalam jaringan harus mempunyai alamat IP unik. Sehingga bila intranet hendak dikoneksikan dengan internet setiap host atau komputer yang dihubungkan harus mempunyai alamat IP yang sesuai dengan aturan pengalamatan yang digunakan dalam internet.

Pengalamatan host yang unik menjadi masalah rumit. Seiring dengan melajunya pertumbuhan manusia di dunia, pengguna

*) Dosen STMIK PPKIA Pradnya Paramita Malang

komputer yang hendak mengkoneksikan dirinya kedalam internet semakin besar jumlahnya. Ini berarti membutuhkan banyak alamat IP. Sedangkan alamat IP yang dapat digunakan jumlahnya terbatas. Masalah tersebut ditambah dengan masalah *routing* yang semakin kompleks. Untuk itu harus ada suatu mekanisme baru untuk memperoleh suatu himpunan alamat IP yang unik.

Dengan terkoneksinya internet dan intranet maka seluruh user dalam intranet dapat mengakses informasi yang berada dalam internet, begitu pula sebaliknya. Sehingga keamanan data intranet dapat terancam bila ada akses langsung dari internet ke intranet. Maka harus ada suatu batasan antara internet dan intranet.

Sebuah perusahaan yang telah menerapkan intranet dan yang akan menghubungkan intranetnya ke dalam internet membutuhkan suatu sistem yang tepat untuk konektifitas intranet-internet yang efisien dan efektif sehingga dapat meningkatkan kinerja perusahaan.

Konsep NAT (*Network Address Translator*) memberikan suatu solusi dalam mengatasi terbatasnya alamat IP yang tersedia. IP *masquereding* adalah layanan pada internet yang merupakan penerapan konsep NAT yang dapat mengurangi permintaan alamat IP baru dalam menghubungkan diri kedalam internet dan dapat meningkatkan keamanan intranet. IP *masquereding* ini merupakan salah satu kemampuan tambahan pada sistem operasi LINUX.

KAJIAN TEORI

1. Konsep NAT dan Layanan IP

Masquereding

Internet telah berkembang menjadi jaringan yang sangat besar dan kompleks sehingga timbul masalah diantaranya kelangkaan untuk mendapatkan alamat IP yang teregistrasi dan masalah *routing* yang semakin kompleks.

Untuk mengatasi hal tersebut dikembangkan protokol dengan versi baru yaitu IPv6 atau IPng (*IP next generation*). IPv6 ini mempunyai panjang alamat IP sebesar 128 bit, sehingga memungkinkan pengalamatan dan *routing* lebih luas. Protokol IPv6 direncanakan menggantikan protokol IPv4 yang masih diapakai oleh seluruh jaringan di dunia. Pergantian protokol IPv4 ke IPv6 sangat sulit dilakukan, memakan waktu lama dan biaya yang sangat besar, karena mengharuskan suatu jaringan mengganti seluruh mekanisme sistem jaringannya, yang meliputi berbagai perangkat keras dan lunak yang kompatibel dengan protokol lama. Semua itu harus dilakukan oleh semua organisasi perusahaan dan host seluruh dunia yang jumlahnya sangat besar. Ditambah lagi dengan pengelolaan internet yang terdistribusi.

Suatu konsep tentang NAT (*Network Address Translator*) ditawarkan sebagai salah satu solusi yang dapat memecahkan masalah

*) Dosen STMIK PPKIA Pradnya Paramita Malang

kelangkaan alamat IP yang teregistrasi. Konsep NAT ini memberikan solusi yang efisien dan efektif kepada seluruh pengguna internet dalam melakukan konektifitasnya dengan memaksimalkan sumber daya yang ada.

NAT diibaratkan sebagai *router* yang mempunyai kemampuan untuk menerjemahkan beberapa alamat IP tidak teregistrasi kedalam 1 alamat teregistrasi jika komunikasi ke internet diperlukan.

NAT akan berperan sebagai *gateway* utama bagi setiap host untuk melakukan koneksi ke internetdengan mengirimkan setiap paket informasi melalui NAT. NAT melakukan modifikasi paket dengan menggunakan mekanisme identifikasi port dan mengganti beberapa informasi port serta alamat IP dalam tiap paket yang datang dari dalam intranet, sehingga koneksi ke internet tersebut seakan berasal dari NAT itu sendiri.

Sebaliknya bila paket balasan datang dari internet untuk salah satu host di dalam intranet, akan diterima lebih dulu oleh NAT untuk melakukan modifikasi terhadap paket atas dasar koneksi yang telah dibuat sebelumnya.

Dengan mengimplementasikan NAT pada intranet, himpunan alamat IP tak teregistrasi yang digunakan oleh suatu intranet dapat dipakai ulang oleh intranet ditempat lain, dan kedua intranet tersebut dapat saling berkomunikasi satu dengan yang lain melalui internet walaupun kedua host yang melakukan koneksi tersebut mempunyai alamat IP tak teregistrasi yang sama.

Dalam internet, himpunan alamat IP tak teregistrasi tidak boleh digunakan di internet karena akan menggangu *routing* dalam internet. LAN lebih mengalokasikan himpunan alamat IP tak teregistrasi yang khusus digunakan untuk hal tersebut. Alokasi alamat IP tersebut didokumentasikan dalam RFG 1597.

2. Prinsip Kerja IP *masquerading*

IP *masquerading* merupakan implementasi kemampuan jaringan konsep NAT tambahan pada operasi Linux. Diaplikasikan mulai dari kernel versi 1.2.13 dan terus mengalami perkembangan sampai kernel versi terakhir (sekarang versi 2.0.36). Dengan menggunakan NAT, IP *masquerading* dapat mengakses internet secara tersamarkan (*masqurade*) dibalik *gateway*.

IP *masquerading* bekerja atas dasar konsep NAT ditambah dengan beberapa fungsi modifikasi hingga tingkat aplikasi yang mulai diterapkan pada kernel versi 2.0.0. Hal ini diwujudkan pada beberapa aplikasi seperti FTP dan IRC, karena aplikasi tersebut mempertukarkan alamat IP atau informasi tertentu yang menyangkut mekanisme *client-server.* Untuk mencegah penumpukan data dalam memori IP *masquerading* membuat batasan waktu koneksi setiap host pada intranet.

Contohnya DNS *client* suatu Host A (192.168.1.3) pada suatu intranet hendak

*) Dosen STMIK PPKIA Pradnya Paramita Malang

membutuhkan pelayanan dari DNS server pada suatu Host B (202.100.10.1) dengan membuka port 53 di internet. Maka DNS *client* tersebut akan membuka suatu port pada host A secara acak (didapat port 1000). Host A kemudian mengirimkan paket AB ke host B melalui layanan IP *masquerading* sebagai *gateway* utama intranet ke internet.

Layanan IP *masquerading* menerima paket AB dan melakukan pencocokan informasi, tapi ternyata cocok sehingga data paket AB dianggap sebagai koneksi baru. Langkah berikutnya layanan IP *masquerading* akan membuka suatu port baru secara acak (didapat port 3800) pada alamat IP teregistrasinya.

Kemudian layanan IP *masquerading* akan melakukan modifikasi pada paket AB yaitu: mengganti alamat IP sumber host A (192.168.1.13) yang tak teregistrasi dengan alamat IP teregistrasi pada layana IP *masquerading* (202.155.1.100) dan mengganti nomor port sumber (port 1000) dengan nomor port sumber baru (port 3800).

Hasil modifikasi paket AB (paket AB-M) dihantarkan ke host B di internet pada port 53. Host B akan menerima paket tersebut sebagai paket yang berasal dari suatu host yang mempunyai alamat IP teregistrasi DNS server (host B) dan akan mengirimkan paket balasan (paket CD) kembali ke alamat sumber (202.155.1.100, port 3800) kemudian dicocokkan. Jika kedua nomor port tersebut berbeda maka paket tersebut akan diabaikan. Tapi jika sama maka IP *masquerading* akan memodifikasi paket CD sebagai berikut: alamat IP tujuan paket (202.155.1.100) diganti dengan alamat IP sumber (host A) dan mengganti nomor port sumber tujuan (port 3800) menjadi port 1000. Paket yang telah dimodifikasi (paket CD-M) akan dihantarkan kembali pada host asal yang memintanya.

Terlihat bahwa mekanisme yang dilakukan oleh layanan IP *masquerading* sangat transparan terhadap host di intranet maupun host di internet. Setiap host dalam intranet menganggap bahwa koneksi ke internet dapat dilakukan melalui layanan IP *masquerading* sebagai *gateway* utama intranet ke internet. Sebaliknya internet akan mengira koneksi yang dibuat berasal dari layanan IP *masquerading*, bukan berasal dari host A. Hal ini menyebabkan intranet selalu tersamarkan dari internet.

Dari segi keamanan data layanan IP *masquerading* bersifat *statefull* karena paket yang diperbolehkan masuk ke intranet adalah paket balasan dari koneksi yang dibuka sebelumnya oleh host dalam intranet. Host di internet tidak bisa membuka koneksi ke dalam intranet. Hal ini merupakan peningkatan keamanan pada intranet atas akses langsung dari internet.

3. Perancangan Sistem Layanan IP *masquerading*

Konfigurasi intranet perusahaan pada awalnya masih sederhana. Semua host

*) Dosen STMIK PPKIA Pradnya Paramita Malang

dihubungkan dengan topologi star pada satu hub. Semua layanan intranet ditumpukkan pada satu server. Karena perusahaan semakin berkembang dan jumlah host pada perusahaan semakin banyak, sistem intranet perusahaan harus diubah sesuai dengan kebutuhan perusahaan.

Sebelum menggunakan layanan IP *masquerading* perusahaan menggunakan *software wingate* untuk melakukan koneksi intranet ke internet. Banyak kendala yang ditemui perusahaan dalam menggunakan *software wingate* ini. Perusahaan memutuskan untuk mengganti sistem konektifitas intranet-internetnya dengan layanan IP *masquerading*.

Untuk memulai membangun sistem layanan IP *masquerading* diperlukan beberapa kebutuhan sebagai suatu konfigurasi dasar. Konfigurasi dasar tersebut adalah sebagai berikut:

- Intranet yang telah dibangun dengan menerapkan pengalamatan sesuai dengan ketentuan dalam dokumen RFC 1597.
- Koneksi internet melalui ISP (*Internet Service Provider*) dengan satu alamat IP teregistrasi.
- Sebuah komputer dengan sistem operasi Linux yang terkonfigurasi dan dapat beroperasi sebagai router. Komputer ini yang akan dimanfaatkan sebagai layanan IP *masquerading*.

Intranet dari satu jaringan utama menghubungkan semua subnet disetiap lantai gedung. Setiap subnet menggunakan sebuah router sebagai penghubung ke jaringan utama (*backbone*) yang menghubungkan ke jaringan luar yang terkoneksi langsung ke internet dengan memanfaatkan layanan IP *masquerading* sebagai *gateway* utama intranet.

Himpunan alamat yang diimplementasikan adalah beberapa jaringan kelas C himpunan alamat IP tek teregistrasi 192.168.1.0 – 192.168.3.255 dengan menggunakna subnet mask 255.255.255.3. Pembagian jaringan kedalam beberapa subnet untuk setiap area dimaksudkan agar terjadi pemisahan arus data pada setiap bagian area dan mempermudah dalam manajemen jaringan. Setiap subnet area mempunyai satu buah router yang menghubungkan jaringan pada setiap area dengan jaringan utama (*backbone*).

Untuk menghubungkan intranet ke internet, perusahaan menggunakan jasa pelayanan internet, ISP Idolanet dengan satu buah mailbox dan satu buah account yang digunakan untuk mengkoneksikan sejumlah komputer yang berada dalam intranet perusahaan. Hal ini berkaitan dengan kesulitan untuk mendapatkan himpunan alamat IP teregistrasi yang memadai untuk seluruh intranet pada saat ini. Selain itu ditinjau dari segi ekonomis, penambahan alamat IP teregistrasi atau penambahan account untuk setiap host di intranet akan memberatkan perusahaan dalam masalah biaya dan tidak efisien.

Untuk membangun layanan IP *masquerading*, konfigurasi dasar yang dibutuhkan harus semuanya terpenuhi. Dalam konfigurasi

*) Dosen STMIK PPKIA Pradnya Paramita Malang

dasar diperlukan sebuah komputer dengan sistem operasi Linux yang telah terkonfigurasi lengkap dan beroperasi sebagai *router*. Dalam komputer tersebut IP *masquerading* diletakkan sebagai layanan IP *masquerading*.

Konfigurasi perangkat keras komputer yang digunakna perusahaan untuk layanan IP *masquerading* yang diimplementasikan pada intranet adalah sebagai berikut:

- IBM PC Server 486 DX4 – 100.
- RAM 32 MB.
- NIC (*Network Interface Card*) NE 2000.

Sistem operasi Linux yang digunakan merupakan distribusi dari SuSE dengan versi 5.3. Dalam SuSE ini sudah terdapat program yang dibutuhkan untuk membangun layanan IP *masquerading*. Namun karena sifat dari sistem operasi Linux yang terus menerus mengalami perkembangan, versi terbaru beberapa program bisa diambil dari internet.

Untuk membangun layanan IP *masquerading* memerlukan beberapa program, yaitu:

- Kernel terbaru versi 2.0.35 atau lebih tinggi dan dapat diperoleh dari http://www.kernel.org dan beberapa site lain.
- Software modul kernel versi 2.0.0 atau lebih untuk mendukung aplikasi internet seperti: FTP, IRC dan lain-lain yang bisa diperoleh di http://www.pi.se/blox/modules/modules/modules-2.0.0 tar.gx.
- Software ipfwadm versi 2.3 atau versi terakhir yang dapat diperoleh di ftp://ftp.xos.nl/pub/linux/ipfwadm-2.3 tar.gz merupakan site utama dari IP *masquerading*.
- Beberapa aplikasi yang mendukung IP *masquerading* bisa didapatkan pada IP *masquerading resource* di http://ipmasq.cjb.net.

Kemmapuan sistem operasi linux sebagai layanan IP *masquerading* berada pada kernel sistem operasi itu sendiri. Kernel merupakan inti dari sistem operasi berupa tata olah dari memori kerja. Kernel linux didistribusikan dalam bentuk kode sumber yang ditulis dalam bahasa C. Untuk melakukan konfigurasi ulang kernel perlu dilakukan proses kompilasi terhadap sumber tersebut.

Dalam distribusi SuSE versi 5.3 sudah terdapat modul penginstalan sistem operasi linux yang mempermudah proses penginstalan. Dalam menu penginstalan menu dapat dipilih tema dari sistem operasi linux yang akan diinstall. Karena komputer yang dibutuhkan berfungsi sebagai server jaringan layanan IP *masquerading* maka dipilih tema internet server. Dalam pilihan tersebut terdapat semua program yang dibutuhkan dalam membangun layanan IP *masquerading* diantaranya:

- Diald (*Program Auto Dial*).

*) Dosen STMIK PPKIA Pradnya Paramita Malang

- Ipfwadn (*IP firewall and Accounting Administration*).
- PPP (*Point to Point protocol*).
- SuSE PPP.

Dalam percobaan implementasi layanan IP *masquerading* pada intranet perusahanaan, kernel yang dimasukkan dalam paket adalah versi 3.0.33. Kernel versi ini sebenarnya sudah mencukupi tetapi agar kernel selalu uptodate dilakukan kompilasi kernel dengan versi 2.0.35 didistribusikan dalam berkas linux 2.0.35 tar.gz.

Kernel tersebut harus diletakkan pada direktori /usr/scr/linux. Kernel linux tersebut didistribusikan dalam berkas termampatkan, sehingga harus dilakukan proses pemekaran. Untuk melakukan proses pemekaran dilakukan langkah sebagai berikut:

cd /usr/scr

tar xzvf linux-2.0.35. tar.gz

Untuk melakukan pencabutan dilakukan akses sebagai pengguna tertinggi (root). Berkas tersebut kemudian tersalin dalam direktori /usr/linux-2.0.35 sehingga perlu dilakukan pembuatan direktori hubung (*link*) sebagai berikut:

ln – s /usr/scr/linux-2.-.35

/usr/src/linux

Kemampuan IP *masquerading* dapat ditambahkan dengan menambahkan beberapa tambahan pada kernel. Penambahan ini dimaksudkan untuk menambah kemampuan IP *masquerading* dan dapat untuk menjalankan aplikasi yang terus berkembang saat ini, sehingga banyak patch baru yang dapat ditambahkan pada IP *masquerading*. Beberapa tambahan yang ditambahkan pada implementasi ini antara lain: icmp_masq2.patch. Patch ini untuk kemampuan tambahan menangani protokol ICMP. Untuk menambahkan pada kernel program tersebut diletakkan pada direktori /usr/src/linux dan dilakukan langkah berikut:

cd/usr/src/linux

patch<icmp_masq2.patch

Langkah berikutnya adalah melakukan konfigurasi pada file .config dengan bantuan program teks editor biasa, beberapa pilihan yang harus dikonfigurasi antara lain:

- config_experimental = y, untuk mendapatkan beberapa dukungan tambahan IP *masquerading* yang sifatnya masih dalam percobaan.
- config_moules = y, untuk mengaktifkan dukungan modul kernel.
- config_net = y, dukungan agar sistem linux dapat beroperasi dalam jaringan.
- config_firewall = y, dukungan dalam penyaringan paket.
- config_inet = y, dukungan protokol TCP/IP pada sistem operasi linux.
- config_ip_forwading = y, untuk memfungsikan sistem operasi linux agar berfungsi sebagai router.
- config_ip_firewall = y, untuk menyaring paket IP.

*) Dosen STMIK PPKIA Pradnya Paramita Malang

- config_ip_masquerade = y, untuk mengaktifkan IP *masquerading*.
- config_ip_always_defrag = y, untuk melakukan defrag.

Proses kompilasi kernel dapat dilakukan dengan bantuan perangkat lunak make sebagai berikut:

#cd/usr/src/linux

#make dep;make clean;make zimage;makezlilo

Bila berhasil maka berkas kernel vm linux yang baru akan berada pada direktori root.

Setelah proses kompilasi kernel tersebut dilaksanakan maka sistem perlu dijalankan ulang agar kernel yang sudah dikompilasi dapat dimuat dalam memori kerja.

Langkah selanjutnya melakukan proses kompilasi dan instalasi terhadap beberapa modul tambahan dengan program bantu make:

#make modules

#make modules_install

Modul yang diinstal pada implementasi ini antara lain:

- ip_masq_ftp untuk apliaksi FTP.
- ip_masq_raufio untuk aplikasi real audio yang berbasis audio.
- ip_masq_irc untuk aplikasi IRC.

Modul tersebut diletakkan pada direktori /lib/modules/2.28/ipv4. Modul yang telah diinstal tersebut harus dipanggil pada saat mesin dijalankan sehingga perlu ditambahkan baris perintah pada file rc.local yang terletak pada direktori /etc/rc.d/ sehingga modul tersebut dipanggil secara otomatis setiap kali mesin dijalankan. Perintah yang harus ditambahkan sesuai dengan modul yang diinstal yaitu:

.
.
/sbin/depmod-a
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
/sbin/modprobe ip_masq_irc
.
.

Pada kernel versi 2.0.34 keatas, IP forwading tidak diaktifkan sehingga perlu dijalankan perintah sebagai berikut:

echo”1”>/proc/sys/net/ipv4 /ip_forwading

atau dengan melakukan perubahan konfigurasi pada /etc/sysconfig/network yaitu:

forward_ipv4 = false menjadi

forward_ipv4 = true

Setelah semua selesai dilakukan maka sistem perlu dijalankan ulang agar kernel yang sudah dikompilasi dapat dimuat dalam memori kerja.

Stelah restart maka hal selanjutnya yang dilakukan adalah melakukan konfigurasi IP address dan Network Device. Konfigurasi dapat dilakukan dengan menggunakan program YaST.

Konfigurasi pada menu YaST dapat dilakukan sebagai berikut: Pada menu utama pilih system administrator → network configuration → network base configuration, kemudian diisi dengan alamat IP address dan network devicenya

*) Dosen STMIK PPKIA Pradnya Paramita Malang

yaitu modem. Dalam menu ini juga diisi alamat ISP, nomor dial, user name dan passwordnya.

Kemudian membuat file config diald. Diald merupakan prgram autodial yang digunakan untuk melakukan dial up ke ISP secara otomatis dari komputer client ketika model dalam keadaan non aktif. Program diald ini akan berada dalam memori dengan bantuan SLIP (*Serial Line Internet Protocol*) diald memonitor permintaan paket TCP/IP dari client, bila ada permintaan maka diald akan melakukan koneksi (*dial up*) secara otomatis ke ISP dengan bantuan protokol PPP. File diald yang dibutuhkan ada dua yaitu:

- diald.conf
- diald.desf

file tersebut dapat dibuat dengan bantuan help file yaitu diald.gz yang berisi konfigurasi yang dibutuhkan dalam melakukan dial up ke ISP.

Untuk menambah performa dari IP *masquerading* dapat digunakan program tambahan *squid*. Dengan program ini IP *masquerading* akan berfungsi sebagai mesin proxy yaitu me-load dan menyimpan file yang diakses oleh host dan apabila ada host yang meminta / mengakses file yang sama maka akan diambil dari file yang telah disimpan dan tidak mengambil dari server asal. Hal ini akan mempercepat akses dan mengurangi lalu lintas jaringan. Program ini dapat diambil di situs http://www.linuxapps.com.

Aturan penerusan paket IP (*IP Forwading Polices*) merupakan aturan yang harus dilakukan oleh *router* ketika menerima, meneruskan / mengeluarkan suatu paket IP. Layanan IP *masquerading* diasumsikan sebagai suatu *router* yang menghubungkan intranet ke internet. Maka layanan IP *masquerading* harus mempunyai atauran penerusan paket tersebut.

Aturan penerusan paket IP dapat dibagi menjadi tiga kelompok menurut bidang kerjanya. Pengelompokan penerusan paket IP adalah sebagai berikut:

1. Aturan terhadap apa yang harus dilakukan ketika ada paket IP yang masuk (*IP Forwading Input Rules*).
2. Aturan terhadap apa yang dilakukan ketika ada paket IP yang keluar (*IP Forwading Output Rules*).
3. Aturan tentang penerusan paket IP *masquerading* (*IP masquerading Rules*).

Untuk menerapkan aturan penerusan paket IP tersebut diperlukan perangkat lunak bantuan ipfwadm (*IP Firewall and Accounting Adminstrator*).

Sebelum melakukan ipfwadm setiap host sudah memiliki nomor sesuai dengan dokumen RFC 1597, dan pengelola jaringan sudah menentukan aturan yang akan diterapkan pada intranet. Setiap host mana saja yang boleh mengakses internet, menerima file, mengirim file ke internet dan sebagainya.

Sebagai contoh penulisan perintah ipfwadm misalkan pengelola jaringan menginginkan host dengan IP address 192.168.1.2

*) Dosen STMIK PPKIA Pradnya Paramita Malang

dan 192.168.1.8 untuk mengakses internet maka dilakukan perintah:

- Ipfwadm –F –a deny.
- Ipfwadm –F –a m –S 192.168.1.2/32 –D 0.0.0.0/0.
- Ipfwadm –F –a m –S 192.168.1/32 – D 0.0.0.0/0.

Dengan menggunakan aturan penerusan paket IP maka koneksi dapat diawasi dan dibatasi. Sehingga koneksi yang dilakukan oleh setiap host dapat dikontrol dengan baik oleh pengelola jaringan.

Selain mengkonfigurasi mesin layanan IP *masquerading* mesin host perlu dilakukan konfigurasi agar dapat melakukan koneksi ke mesin layanan IP *masquerading*. Konfigurasi pada mesin host tergantung pada sistem operasi yang digunakan seperti Windows 3.11, Windows 9.x, Windows NT, Unix, Dos, OS/2 atau dengan mesin lain seperti MAC.

Contohnya pada Windows 9x, pada TCP/IP properties, alamat IP host diset menjadi 192.168.1.x dan subnet mask 255.255.255.0 dan gateway diset ke alamat IP layanan *masquerading* 192.168.1.1 setelah dilakukan restart ulang. Kemudian pada apliaksi misalkan web browser pada pilihan koneksi dipilih koneksi dengan menggunakan LAN. Untuk mengecek hubungan dpat digunakan program ping ke mesin layanan IP *masquerading*.

4. Uji Coba Layanan IP *masquerading*

Setelah semua konfigurasi dasar dan layanan IP *masquerading* sudah berhasil dibangun maka langkah terakhir adalah mencoba akses intranet ke internet atau sebaliknya dengan aplikasi internet yang sudah umum digunakan.

Uji coba ini dilakukan dari dalam intranet pada salah satu host dengan menggunakan PC dengan sistem operasi MS Windows 98. Dalam uji coba tersebut dilakukan simulasi beberapa user melakukan koneksi ke internet secara bersamaan.

Aplikasi internet yang digunakan dalam ujicoba tersebut antara lain: internet explorer 4.0, Microsoft Outlook dan PING.

5. Uji Coba Aplikasi WWW

WWW (*World Wide Web*) atau web merupakan salah satu aplikasi yang disediakan dalam internet. Dalam www, disajikan informasi dalam bentuk format dokumen HTML (*Hyper Text Markup Language*). Untuk mengakses dokumen tersebut diperlukan program web browser. Dalam ujicoba ini digunakan web browser: Internet Explorer 4.0 dari Microsoft.

6. Uji Coba Aplikasi E-mail

Untuk mengirim e-mail dalam internet digunakan SMTP (*Simple Mail Transfer Protocol*) dan untuk menerima e-mail digunakan POP (*Post Office Protocol*). Perangkat lunak yang digunakan untuk mengirim, menerima dan membaca e-mail

*) Dosen STMIK PPKIA Pradnya Paramita Malang

yang digunakan dalam uji coba ini adalah Microsoft Outlook.

7. Uji Coba Aplikasi PING

Untuk mendeteksi jaringan terhubung dengan baik digunakan program bantu PING (*Packet Inter Net Gopher*). Aplikasi ini berbasiskan protocol ICMP. PING akan mengirimkan paket test ke host tujuan bila host tersebut diterima maka paket akan dikirim kembali ke host asal menandakan paket telah diterima dengan baik.

8. Ujia Coba Pengaksesan Intranet dari Luar (*Internet*)

Dalam uji coba ini digunakan komputer yang berada diluar intranet perusahaan dan mengkoneksikannya dengan internet melalui salah satu ISP. Dengan program bantu PING dicoba dilakukan koneksi dengan salah satu host di dalam intranet dengan alamat tak teregistrasi. Dalam uji coba ini komputer mencoba melakukan koneksi ke host 192.168.2.2 pada intranet.

Terlihat bahwa host yang dituju tidak dapat dikoneksi karena alamat tersebut tidak digunakan dalam internet sesuai dengan dokumen RFC 1597 sehingga host di internet tidak dapat melakukan hubungan langsung dengan host didalam intranet. Hal ini menunjukkan bahwa dengan menggunakan layanan IP *masquerading* dapat meningkatkan keamanan intranet.

Berdasarkan uji coba yang telah dilakukan dapat diambil beberapa bahasan mengenai implementasi layanan IP *masquerading*:

1. Layanan IP *masquerading* dapat mengkoneksikan setiap host pada intranet dengan internet dengan menggunakan almaat IP tak teregistrasi.
2. Mekanisme modifikasi paket yang dilakukan layanan IP *masquerading* bersifat transparan bagi host di internet dan intranet.
3. Setiap koneksi dari host dalam intranet ke internet akan dianggap berasal dari layanan IP *masquerading* bukan dari host dalam intranet. Sehingga alamat IP host pada intranet akan tersamarkan.
4. Paket yang diperbolehkan masuk ke dalam intranet adalah paket balasan dari koneksi yang telah dibuat sebelumnya oleh host dalam intranet. Sehingga layanan IP *masquerading* bersifat *statefull* yang akan meningkatkan keamanan intranet.
5. Layanan IP *masquerading* mampu melayani koneksi yang dibuat oleh aplikasi berbasiskan protokol UDP, TCP maupun ICMP. Contoh apliaksi tersebut antara lain DNS, WWW dan PING.
6. Layanan IP *masquerading* dapat melakukan analisis hingga tingkat aplikasi dengan memanfaatkan modul tertentu. Hal

*) Dosen STMIK PPKIA Pradnya Paramita Malang

ini ditujukan dalam uji coba aplikasi FTP dan IRC.

7. Program IP *masquerading* merupakan program yang berada pada lapisan network layers sehingga banyak fungsi yang dapat dijalankan oleh IP *masquerading* seperti firewall, proxy memonitor client dan memantau traffic TCP/IP.
8. Layanan IP *masquerading* tidak memerlukan konfigurasi hardware yang tinggi. Dengan menggunakan IBM PC 486 layanan IP *masquerading* dapat dibangun dan berjalan dengan baik.
9. Program yang dibutuhkan untuk membangun layanan IP *masquerading* maupun sistem operasi linux dapat diperoleh secara gratis dalam internet sehingga IP *masquerading* tidak memerlukan biaya besar dalam membangunnya.
10. Dengan menggunakan layanan IP *masquerading* perusahaan hanya membutuhkan satu buah koneksi (*account*) di internet satu line telpon dan satu buah modem untuk menghubungkan semua host intranetnya untuk melakukan koneksi ke internet.

Dalam implementasi layanan IP *masquerading* terdapat kelemahan atau kesulitan yaitu:

1. Kesulitan dalam hal penginstalan IP *masquerading*, karena sistem operasi yang digunakan berbeda dengan linux yang masih relatif baru bagi kebanyakan user kita sehingga butuh waktu dan ketekunan untuk mempelajari sistem operasi tersebut.
2. Tidak semua aplikasi dapat berjalan dengan layanan IP *masquerading* dan beberapa aplikasi memerlukan file tambahan untuk dapat dijalankan melalui layanan IP *masquerading*.
3. Program ipfwadm masih menggunakan tampilan text base sehingga user akan sedikit kesulitan untuk menggunakan program tersebut.
4. Bila kernel dari sistem operasi linux tersebut diupgrade menjadi versi yang lebih tinggimaka diperlukan file IP *masquerading* dengan versi yang baru pula dan memerlukan konfigurasi ulang.

Berikut perbandingan antara perangkat lunak *wingate* dengan layanan IP *masquerading*:

- Sistem operasi yang digunakan perangkat lunak *wingate* bekerja pada sistem operasi windows yang menggunakan modus GUI (*Graphics User Interface*) untuk pengoperasiannya sehingga sangat membutuhkan *resources* yang besar dan akan memperlambat akses. Sedangkan IP *masquerading* menggunakan sistem operasi linux yang menggunakan modus

*) Dosen STMIK PPKIA Pradnya Paramita Malang

text, perintah dilakukan dengan perintah dasar sehingga menghemat *resources*. Tetapi linux juga memiliki kemampuan untuk modus grafik. Dari segi user friendly memang lebih mudah menggunakan GUI tetapi dari segi performance modus teks akan lebih cepat.

- Sistem yang digunakan, perangkat lunak *wingate* merupakan mesin proxy yang akan menyimpan dokumen / file internet dalam cache memori setiap permintaan dari host sehingga *wingate* memerlukan spesifikasi hardware yang tinggi untuk meload file internet dan menyimpannya dalam memori / harddisk. Layanan IP *masquerading* menggunakan konsep NAT. Dimana alamat IP *masquerading* tak teregistrasi diterjemahkan menjadi alamat IP teregistrasi sehingga dapat disimpan dalam sebuah tabel. Layanan IP *masquerading* hanya bertugas untuk menterjemahkan alamat IP dan memelihara tabel sehingga tidak memerlukan *resources* yang terlalu besar. Layanan IP *masquerading* juga dapat berfungsi sebagai mesin proxy dengan tambahan perangkat lunak squid dengan penampilan yang lebih baik.
- Instalasi perangkat lunak. *Wingate* memerlukan instalasi dan konfigurasi pada host dan server. Server harus diinstal *wingate* server dan setiap host harus diinstal *wingate* internet client. Suatu intranet dapat memiliki jumlah host yang besar, instalasi *wingate* internet client untuk setiap host akan memakan banyak sehingga tidak efisien. IP *masquerading* hanya memerlukan instalasi pada server layanan IP *masquerading* dan host hanya perlu mensetting IP address *gateway* ke server IP *masquerading*. Host dapat menggunakan perangkat lunak yang dipilih sesuai dengan kebutuhan baik itu dalam modus GUI maupun modus teks.

Dari beberapa perbedaan diatas dapat disimpulkan bahwa IP *masquerading* memiliki kelebihan dalam melakukan layanan konektifitas intranet-internet. IP *masquerading* dapat memberikan layanan yang efisien dan efektif yang sesuai dengan kebutuhan perusahaan dalam meningkatkan kinerja dan daya saing perusahaan.

Kesimpulan

Dengan melihat hasil uji coba implementasi layanan IP *masquerading* yang telah diterapkan pada intranet sebuah perusahaan dapat diambil beberapa kesimpulan sebagai berikut:

Digunakannya himpunan alamat IP tak teregistrasi pada intranet dengan memanfaatkan layanan IP *masquerading* sesuai dengan aturan dalam dokumen RFC 1597 maka masalah kelangkaan alamat IP teregistrasi dapat diatasi oleh pengelola jaringan.

*) Dosen STMIK PPKIA Pradnya Paramita Malang

Implementasi layanan IP *masquerading* pada intranet yang menggunakan konsep NAT menyebabkan identitas setiap host dalam intranet selalu tersamarkan dengan alamat layanan IP *masquerading*. Selain itu layanan IP *masquerading* bersifat *statefull* karena paket balasan dari internet yang diperbolehkan masuk adalah paket balasan dari koneksi yang dibuat dari dalam intranet.

Dalam membangun layanan IP *masquerading* ini tidak memerlukan biaya besar karena perangkat lunak yang dibutuhkan dalam membangun layanan IP *masquerading* ini dapat diperoleh secara gratis dan legal di internet, dan tidak memerlukan konfigurasi hardware yang tinggi. Perusahaan hanya membutuhkan satu buah koneksi (*account*) di internet, satu line telpon dan satu buah modem untuk menghubungkan semua host intranetnya untuk melakukan koneksi ke internet. Sehingga layanan IP *masquerading* ini merupakan pilihan yang ekonomis dan efisian dalam membangun layanan konektifitas intranet ke internet.

DAFTAR PUSTAKA

Andoko, Andrey. 1996. *Dari Intranet ke Ekstranet*. Kompas, Rabu 15 Januari.

Au, Ambrose. 2011. *Linux* IP *masquerading Mini Howto*. http://ipmasq.cjb.net. 7 Februari.

Commers, D.E. 1994. *Internetworking With TCP/IP, Principles, Protocols and Architecture*. Prentice Hall Inc, New Jersey.

Evegang, Kjeld dan Francis, Paul. 1994. *The IP Network Address Translator (NAT), RFC 1631, Cray Communication*. NTT.

Hasesnstein, Michael. 2011. *IP Network Address Translation*. http://www.csn.tuchemnitz.de/HyperNews/get/linux-ip-nat.html.

Parker, Timothy. 1994. *Teach Yourself TCP/IP in 14 Days*. Sam Publishing. Indiana.

Warsono. 2010. *Memahami IP Address dan Menentukan Subnetting Pada IPv4*. http://www.jakarta.linux.or.id/artikel/ipv4.html. 11 Desember.

*) Dosen STMIK PPKIA Pradnya Paramita Malang