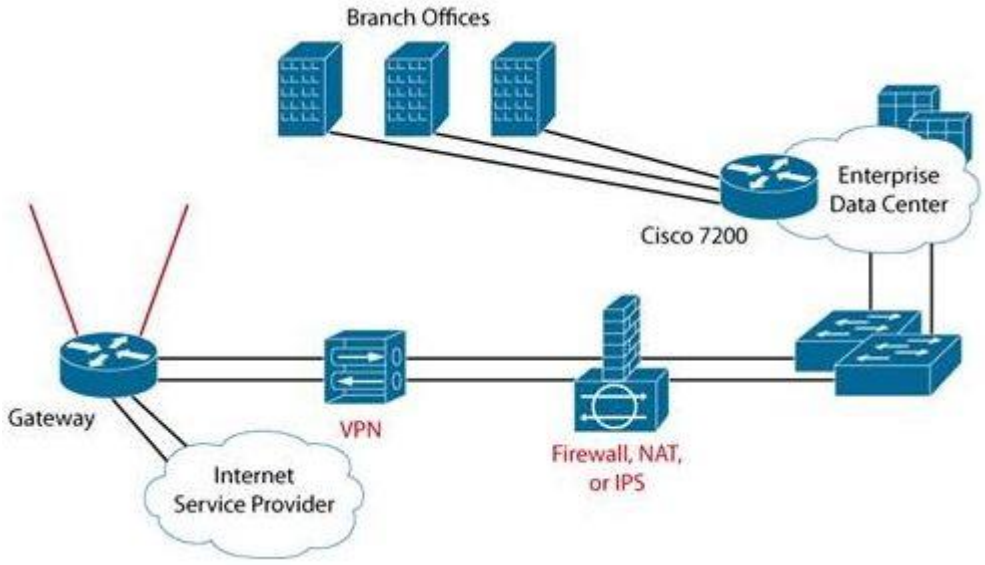
3.8 A. Internet Gateway (NAT)

1. Pengertian Internet Gateway (NAT)

NAT (Network Address Translation) merupakan sebuah proses pemetaan alamat IP dengan perangkat jaringan komputer akan memberikan alamat IP public ke perangkat jaringan lokal. Sehingga, banyak IP privat (IP yang biasa digunakan dalam jaringan yang tidak terhubung ke internet tetapi melalui NAT) yang dapat mengakses IP publik. Artinya, NAT akan mentranslasikan alamat IP sehingga IP address pada jaringan lokal dapat mengakses IP publik pada jaringan WAN. NAT mentranslasikan alamat IP privat untuk dapat mengakses alamat host di internet dengan menggunakan alamat IP publik pada jaringan tersebut. Tanpa hal tersebut (NAT), tidak mungkin IP privat pada jaringan lokal bisa mengakses internet Sebagaimana Anda ketahui bahwa alamat IP publik saat ini sudah makin menipis, sehingga penggunaan data NAT dapat dianggap sangat efisien dan efektif, terutama dalam alokasi alamat IP.

NAT menggabungkan lebih dari satu komputer untuk dihubungkan ke dalam jaringan internet hanya dengan menggunakan sebuah alamat IP. Setiap komputer di dalam NAT ketika berselancar di internet akan terlihat memiliki alamat IP yang sama jika dilacak. Dengan kata lain, sebuah alamat IP pada jaringan lokal akan terlebih dahulu ditranslasikan oleh NAT untuk dapat mengakses IP publik di jaringan komputer. Sebelum proses translasi ini, pengguna tidak dapat terhubung ke internet. Banyak yang berpendapat bahwa NAT hampir sama dengan proxy server. Namun keduanya berbeda. Pada proxy server disediakan mekanisme caching sedangkan pada NAT tidak demikian



Penggunaan NAT, tidak ada batasan mengenai jumlah halaman web dapat diakses. Oleh karena itu, banyak pengguna NAT yang memanfaatkan site ini, karena ketersediaan alamat IP yang terbatas data, membutuhkan keamanan lebih. Selain itu, ada pula yang menggunakan NAT karena dinilai lebih fleksibe dalam hal administrasi jaringan, sebab jaringan NAT didesain menyederalamat IP dan untuk melindunginya.

2. Prinsip dan Cara Kerja Internet Gateway (NAT)

Pada jaringan komputer, NAT berfungsi sebagai translasi sebuah IP address sehingga dengan adanya NAT ini IP address privat dapat dengan mudah men alamat IP publik Pada IP address, terdapat sebuah bagian yang berisi informasi-informa berupa alamat asal, alamat tujuan. TTL dan lain-lain. Bagian ini disebut header. Berikut cara kerja dari NAT. Misalkan sebuah komputer client dengan IP 192.168.1.2 akan mengakses atau melakukan request ke alamat dengan IP 21623938120 D

1) Pada header informasi yang tersimpan antara lain alamat asal > 192.168.1.2 2)

2) Ketika paket telah sampai pada router (gateway dari client), maka ia dari header akan diubah menjadi alamat asal > 192.168.1.1

3) Sebelum paket keluar (menuju internet), maka header tersebut akan kembali berubah menjadi alamat asal > 200100502 demikian seterusnya.

Proses di atas merupakan mekanisme dari SNAT (source NAT), dengan IP

asal komputer client) akan diubah disesuaikan dengan IP ketika paket telah berpindah. Ketika server google melakukan respons/balasan, maka akan terjadi DNAT (destination NAT), dengan IP tujuan akan berubah disesuaikan dengan tujuan paket (komputer client). Prosesnya adalah sebagai berikut.

1) Pada header, ketika paket telah sampai pada router, informasi IP tujuann > 2001005020

2) Ketika paket berada pada gateway, IP tujuan > 19216811

3) Di sini header akan kembali mengalami perubahan, IP tujuan > 192.168.1.2

4) Paket dapat dikirim dan bisa sampai pada komputer client.

3. Jenis-Jenis Internet Gateway (NAT)

Ada empat jenis NAT yang perlu diketahui, yaitu NAT tipe statis, dinamis, overloading, dan overlapping. Keempat jenis internet gateway terdapat perbedaan Untuk lebih memahaminya, perhatikan uraian berikut.

1. NAT Statis

Bekerja dengan menerjemahkan semua alamat IP yang belum terdaftar menjadi alamat IP yang terdaftar. NAT statis banyak digunakan untuk komputer yang ingin dapat diakses dari luar. NAT statis dapat dikatakan pemborosan terhadap alamat IP yang didaftarkan sebab setiap satu komputer dipetakan untuk satu alamat IP terdaftar, sehingga jika ada banyak komputer yang didaftarkan, tentu makin terbatas pula alamat IP yang masih tersedia.

Kekurangan lain dari NAT statis adalah kurang aman dibandingkan NAT

dinamis, sebab setiap komputer memiliki alamat IP tersendiri, dan akhirnya risiko

penyusup masuk langsung ke dalam jaringan privat lebih besar.

. NAT Dinamis Selain NAT statis, terdapat

b. NAT dinamis.

Berbeda dengan NAT statis, NAT dinamis bekerja dengan mendaftarkan beberapa komputer ke dalam satu kelompok dengan alamat IP terdaftar yang sama. Nantinya, ada beberapa komputer yang memiliki kesamaan alamat IP terdaftar.

Fungsi GATEWAY

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan computer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda.

Istilah gateway merujuk kepada hardware atau software yang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga data dapat ditransfer antar komputer yang berbeda-beda. Salah satu contoh penggunaan gateway adalah pada email, sehingga pertukaran email dapat dilakukan pada sistem yang berbeda.

Host yang digunakan untuk mengalihkan lalu lintas jaringan dari satu jaringan ke jaringan lain, juga digunakan untuk melewatkan lalu lintas jaringan dari satu protokol ke protokol lain. Dipergunakan untuk menghubungkan dua jenis jaringan komputer yang arsitekturnya sama sekali berbeda. Jadi gateway lebih kompleks daripada bridge.

Gateway dapat diaplikasikan antara lain untuk menghubungkan IBM SNA dengan digital DNA, LAN (Local Area Network) dengan WAN (Wide Area Network). Salah satu fungsi poko gateway adalah melakukan protocol converting, agar dua arsitektur jaringan komputer yang berbeda dapat berkomunikasi.

Gateway juga bisa diartikan sebagai komputer yang memiliki minimal 2 buah network interface untuk menghubungkan 2 buah jaringan atau lebih. Di Internet suatu alamat bisa ditempuh lewat gateway-gateway yang memberikan jalan/rute ke arah mana yang harus dilalui supaya paket data sampai ke tujuan. Kebanyakan gateway menjalankan routing daemon (program yang meng-update secara dinamis tabel routing). Karena itu gateway juga biasanya berfungsi sebagai router. Gateway/router bisa berbentuk Router box seperti yang di produksi Cisco, 3COM, dll atau bisa juga berupa komputer yang menjalankan Network Operating System plus routing daemon. Misalkan PC yang dipasang Unix FreeBSD dan menjalankan program Routed atau Gated. Namun dalam pemakaian Natd, routing daemon tidak perlu dijalankan, jadi cukup dipasang gateway saja.

Cara Setting IP Address Dalam Komputer Jaringan Gateway

CaraSetting Mikrotik RouterOS PPPoE Client Sebagai Gateway Telkom Speedy. Dengan jaringan komputer yang baik tentu jaringan internet pasti lebih kenceng. Setup modem adsl anda sebagai bridge protocol mode. Settingnya dapat anda temukan dari manual masing-masing modem Biasanya setting bridging protocol pada beberapa modem, ada pada menu Advance setup > WAN. Kemudian lakukan save/reboot. Selesai setting modem sebagai bridging (password dan user ID tidak tersimpan dimodem). Bagi yang ingin mengganti IP address default modem bisa di konfigurasi terlebih dahulu melalui PC client.

Caranya : Masuk ke ke modem melalui browser dan masuk ke menu (biasanya) Advance Setup > LAN IP Address Contoh 192.168.1.1 lakukan save/reboot. (sekarang IP modemnya adalah 192.168.1.1) Kemudian lakukan pengubahan IP juga pada komputer client (tempat anda melakukan setup modem) menjadi (misalnya) 192.168.1.2 selesai. Buka browser dan coba ketik IP modem (192.168.1.1). Berhasil? Kita lanjut ke CPU Mikrotik RouterOS nya. Tentukan IP Address masing-masing LAN card anda. (dibutuhkan minimal 2 LAN Card pada komputer yang akan dipasangi mikrotik) Card LAN yang akan ke modem 192.168.1.2 (PUBLIK) Card LAN yang akan dimasukkan ke hub/switch untuk jaringan lokal 192.168.10.254 (LAN). Semua perintah yang kita ketikkan disini berbasis text (text mode) dan dilakukan di mesin mikrotiknya Agar tidak bingung, Lakukan perintah untuk memberi nama masing2 Card Ethernet tadi. Memberi nama pada masing2 Card Jaringan >interface ethernet set ether1 name=PUBLIK >interface ethernet set ether2 name=LAN Setting IP Address untuk masing2 Card Lan tadi /ip address add address=192.168.1.2/24 interface=PUBLIK /ip address add address=192.168.10.254/24 interface=LAN Memasukkan entry PPPoE Client. Perintah ini sudah bisa dilakukan lewat klien dan menggunakan Winbox/ gui) /interface pppoe-client add name=pppoe-user-telkom user=telkom password=123@telkom interface=PUBLIK service-name=Internet disabled=no (username dan password cuman perumpamaan) Gateway — Routingnya dan masquerading /ip route add gateway= 125.167.122.1 (IP Gateway Telkom bukan IP yang static kita) IP gateway diatas belum tentu sama, lihat terlebih dahulu ip pppoe client anda. Jika anda belum yakin 100% ip client anda dan gateway nya, lakukan login dan dialing melalui modem anda terlebih dahulu bukan pada mode bridging seperti diatas. Pada menu Device Info akan tampil informasi Default Gateway dan IP client pppoe anda. Selanjutnya Masquerading, untuk penerusan perintah dari routing yang diteruskan ke NAT Firewall mikrotik untuk proses routing ke semua client yang terkoneksi /ip firewall nat add chain=srcnat action=masquerade out-interface=internet Setting DNS dengan perintah di terminal winbox. /ip dns set primary-dns=202.134.1.10 /ip dns set primary-dns=203.130.206.250 /ip dns allow-remote-request=yes Selesai.. tahap routing sudah terlaksanakan. Coba lakukan ping ke mikrotik dan gateway nya. Jika anda ingin sharing ke komputer client jangan lupa masukkan ip gateway pada settingan Network Connection (windows) sesuai dengan IP LAN (192.168.10.254) pada mikrotik anda.

Banyak sekali settingan mikrotik yang dapat anda pelajari dari berbagai sumber. Jika terkesan terlalu rumit dengan sistem pengetikan anda bisa melakukannya dengan winbox mode, setiap tutorial yang anda butuhkan pun dapat anda copy dan paste ke winbox nya mikrotik. Setting Web Proxy Transparant /ip web-proxy set enabled=yes port=8080 hostname=dipanegara.

proxy transpa rent-proxy=yes
/ip firewall nat add in-interface=lokal dst-port=80 protocol=tcp action=redirect to-ports=8080 chain=dstnat dst-address=!192.168.10.254/24 (portnyas bisa kita tentukan sendiri misalnya 3128 dll)
Jangan lupa untuk menset IP gateway client anda ke 192.168.10.254 agar terkoneksi ke server mikrotik
Demikian tutorial singkat jaringan komputer mikrotik sebagai gateway koneksi ke speedy dgn metode Bridging.
JIka terjadi masalah, biasanya ada pada setting gateway, untuk itu bisa dicoba menambahkan perintah pada :
/interface pppoe-client add name=pppoe-user-telkom user=telkom password=123@telkom.net interface=public service-name=internet disabled=no add-default-route=yes
sumber: wahyuheri.wordpress.com
Dengan cara setting jaringan komputer gateway speedy diatas bisa mempercepat kecepatan download kita
Cara setting DNS Server dalam komputer jaringan
Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan computer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda. Definisi tersebut adalah definisi gateway yang utama.

Seiring dengan merebaknya internet, definisi gateway seringkali bergeser. Tidak jarang pula pemula menyamakan “gateway” dengan “router” yang sebetulnya tidak benar.

Kadangkala, kata “gateway” digunakan untuk mendeskripkan perangkat yang menghubungkan jaringan komputer besar dengan jaringan komputer besar lainnya. Hal ini muncul karena seringkali perbedaan protokol komunikasi dalam jaringan komputer hanya terjadi di tingkat jaringan komputer yang besar.

KEUNTUNGAN DAN KERUGIAN

MENGGUNAKAN GATEWAY PADA JARINGAN KOMPUTER

A. KEUNTUNGAN

1. Resource Sharing, dapat menggunakan sumberdaya yang ada secara bersamasama. Misal seorang pengguna yang berada 100 km jauhnya dari suatu data, tidak mendapatkan kesulitan dalam menggunakan data tersebut, seolah-olah data tersebut berada didekatnya. Hal ini sering diartikan bahwa jaringan komputer mangatasi masalah jarak.

2. Reliabilitas tinggi, dengan jaringan komputer kita akan mendapatkan reliabilitas yang tinggi dengan memiliki sumber-sumber alternatif persediaan. Misalnya, semua file dapat disimpan atau dicopy ke dua, tiga atu lebih komputer yang terkoneksi kejaringan. Sehingga bila salah satu mesin rusak, maka salinan dimesin yang lain bisa digunakan.

3. Menghemat uang, Komputer berukutan kecil mempunyai rasio harga/kinerja yang lebih baik dibandingkan dengan komputer yang besar. Komputer besar seperti mainframe memiliki kecapatan kira-kira sepuluh kali lipat kecepatan komputer kecil/pribadi. Akan

tetap, harga mainframe seribu kali lebih mahal dari komputer pribadi. Ketidakseimbangan rasio harga/kinerja dan kecepatan inilah membuat para perancang sistem untuk membangun sistem yang terdiri dari komputer-komputer pribadi.

4. Hardware sharing, Bagi pakai hardware secara bersama-sama. Dengan adanya fasilitas jaringan kemudian menggunakan alat yang bernama printer server. maka sebuah printer laser berwarna yang mahal sekali harganya dapat dipakai secara bersama-sama oleh 10 orang pegawai. Begitu pula halnya dengan scanner, Plotter, dan alat-alat lainnya.

5. Keamanan dan pengaturan data, komputer dalam sebuah lingkungan bisnis, dengan adanya jaringan tersebut memungkinkan seorang administrator untuk mengorganisasi data-data kantor yang paling penting. Dari pada setiap departemen menjadi terpisah-pisah dan data-datanya tercecer dimana-mana. Data penting tersebut dapat di manage dalam sebuah server back end untuk kemudian di replikasi atau dibackup sesuai kebijakan perusahaan. Begitu pula seorang admin akan dapat mengontrol data-data penting tersebut agar dapat diakses atau di edit oleh orang-orang yang berhak saja.

6. Ke-stabilan dan Peningkatan performa komputasi, Dalam kondisi tertentu, sebuah jaringan dapat digunakan untuk meningkatkan performa keseluruhan dari aplikasi bisnis, dengan cara penugasan komputasi yang di distribusikan kepada beberapa komputer yang ada dalam jaringan.

B. KERUGIAN

1. Biaya yang tinggi kemudian semakin tinggi lagi. pembangunan jaringan meliputi berbagai aspek: pembelian hardware, software, biaya untuk konsultasi perencanaan jaringan, kemudian biaya untuk jasa pembangunan jaringan itu sendiri. Infestasi yang tinggi ini tentunya untuk perusahaan yang besar dengan kebutuhan akan jaringan yang tinggi. Sedangkan untuk pengguna rumahan biaya ini relatif kecil dan dapat ditekan. Tetapi dari awal juga network harus dirancang sedemikian rupa sehingga tidak ada biaya overhead yang semakin membengkak karena misi untuk pemenuhan kebutuhan akan jaringan komputer ini.

2. Manajemen Perangkat keras Dan Administrasi sistem : Di suatu organisasi perusahaan yang telah memiliki sistem, administrasi ini dirasakan merupakan hal yang kecil, paling tidak apabila dibandingkan dengan besarnya biaya pekerjaan dan biaya yang dikeluarkan pada tahap implementasi. Akan tetapi hal ini merupakan tahapan yang paling penting. Karena Kesalahan pada point ini dapat mengakibatkan peninjauan ulang bahkan konstruksi ulang jaringan. Manajemen pemeliharaan ini bersifat berkelanjutan dan memerlukan seorang IT profesional, yang telah mengerti benar akan tugasnya. Atau paling tidak telah mengikuti training dan pelatihan jaringan yang bersifat khusus untuk kebutuhan kantornya.

3. Sharing file yang tidak diinginkan : With the good comes the bad, ini selalu merupakan hal yang umum berlaku (ambigu), kemudahan sharing file dalam jaringan yang ditujukan untuk dipakai oleh orang-orang tertentu, seringkali mengakibatkan bocornya sharing folder dan dapat dibaca pula oleh orang lain yang tidak berhak. Hal ini akan selalu terjadi apabila tidak diatur oleh administrator jaringan.

4. Aplikasi virus dan metode hacking : hal-hal ini selalu menjadi momok yang menakutkan bagi semua orang, mengakibatkan network down dan berhentinya pekerjaan. Permasalahan

ini bersifat klasik karena system yang direncanakan secara tidak baik. Masalah ini akan dijelaskan lebih lanjut dalam bab keamanan jaringan.

NAT(Network Address translation)

Network Address Translation atau yang lebih biasa disebut dengan NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas dalam administrasi jaringan.

Alamat IP

Saat ini, protokol IP yang banyak digunakan adalah IP versi 4 (IPv4). Dengan panjang alamat 4 byte berarti terdapat 2 pangkat 32 = 4.294.967.296 alamat IP yang tersedia. Jumlah ini secara teoretis adalah jumlah komputer yang dapat langsung koneksi ke internet. Karena keterbatasan inilah sebagian besar ISP (Internet Service Provider) hanya akan mengalokasikan satu alamat untuk satu penggna dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet. Hal ini akan menyulitkan untuk bisnis golongan menengah ke bawah. Di satu sisi mereka membutuhkan banyak komputer yang terkoneksi ke internet, akan tetapi di sisi lain hanya tersedia satu alamat IP yang berarti hanya ada satu komputer yang bisa terkoneksi ke internet. Hal ini bisa diatasi dengan metode NAT. Dengan NAT gateway yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dibagi ke beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

Sejarah NAT

Pada pertengahan tahun 1990-an menjadi popular. NAT alat untuk mengurangi dengan alamat IPv4 kelelahan. Hal ini telah menjadi standar, sangat diperlukan dalam fitur router untuk rumah dan kantor kecil koneksi Internet.

Kebanyakan sistem menggunakan NAT melakukannya untuk mengaktifkan beberapa host pada jaringan pribadi untuk mengakses Internet dengan menggunakan satu alamat IP publik (lihat gateway). Namun, pada awalnya NAT breaks envisioned model IP end-to-end konektivitas di Internet, memperkenalkan komplikasi dalam komunikasi antar host memiliki kinerja dan dampak. NAT obscures jaringan internal dari struktur: semua lalu lintas muncul ke pihak luar seperti itu berasal dari mesin gateway.
Jaringan alamat terjemahan melibatkan kembali menulis sumber dan / atau tujuan alamat IP dan biasanya juga TCP / UDP port jumlah IP paket karena lulus melalui NAT. Checksum (keduanya IP dan TCP / UDP) juga harus ditulis ulang untuk mengambil rekening perubahan.

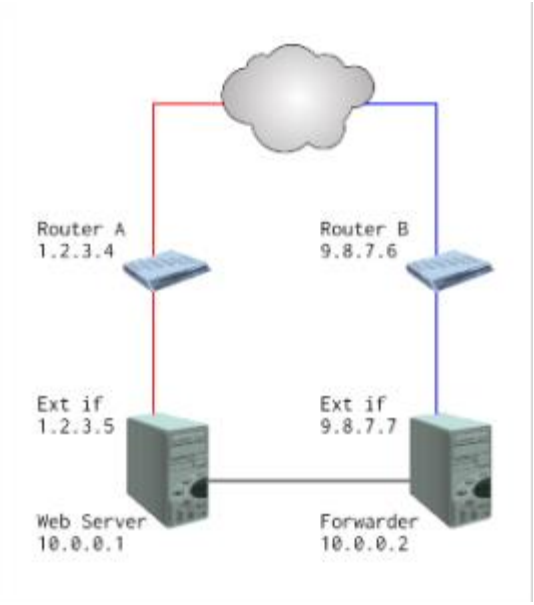
Khas dalam konfigurasi jaringan lokal yang menggunakan salah satu yang “swasta” alamat IP subnets (di RFC 1918). Private Network Alamat adalah 192.168.xx, 172.16.xx melalui 172.31.xx, dan 10.xxx (atau menggunakan notasi CIDR, 192.168/16, 172.16/12, dan 10 / 8), dan router pada jaringan yang memiliki alamat pribadi (seperti 192.168.0.1) di ruang alamat. Router juga terhubung ke Internet dengan satu “publik” alamat (dikenal sebagai “kelebihan beban” NAT) atau beberapa “publik” alamat yang ditetapkan oleh ISP. Karena lalu lintas lolos dari jaringan lokal ke Internet, alamat sumber di masing-masing paket diterjemahkan dengan cepat dari alamat pribadi untuk umum alamat (es).

Router trek data dasar tentang setiap sambungan aktif (terutama alamat dan port tujuan). Ketika sebuah balasan kembali ke router, menggunakan sambungan data pelacakan itu tersimpan selama fase outbound untuk menentukan di mana di jaringan internal untuk meneruskan balasan; dengan TCP atau UDP client port yang digunakan untuk nomor demultiplex paket yang dalam hal keberatan NAT, atau alamat IP dan nomor port ketika beberapa alamat publik yang tersedia, pada paket kembali. Untuk sistem di Internet, router itu sendiri tampil sebagai sumber / tujuan untuk lalu lintas.

Jenis-jenis NAT

NAT terdapat 2 jenis yaitu SNAT dan DNAT

❖ Penggunaan istilah SNAT bervariasi oleh vendor. Banyak vendor ada definisi eksklusif untuk SNAT. Umum adalah definisi Sumber NAT, di banding Tujuan dari NAT (DNAT). Microsoft menggunakan istilah untuk NAT Aman, berkaitan dengan perpanjangan ISA Server dibahas di bawah ini. Per Cisco Systems, SNAT berarti Stateful NAT. The Internet Engineering Task Force (IETF) mendefinisikan SNAT sebagai Softwires Network Address Translation. Ini adalah jenis NAT bernama setelah Softwires kelompok kerja yang diisi dengan standarisasi discovery, dan metode encapsulation untuk menghubungkan jaringan di IPv4 dan IPv6 jaringan IPv6 di jaringan IPv4 jaringan.



❖ Dynamic NAT, seperti NAT statis, tidak umum dalam jaringan yang lebih kecil tetapi lebih besar ditemukan di kompleks perusahaan dengan jaringan. Cara dinamis dari beberapa NAT statis NAT adalah tempat yang statis NAT menyediakan satu-ke-satu ke publik internal static IP pemetaan, Dynamic NAT tidak sama tetapi tanpa membuat pemetaan kepada publik IP statis dan biasanya menggunakan grup umum yang tersedia IP.

Tujuan DNAT adalah teknik transparan untuk tujuan mengubah alamat IP dari id-rute paket dan melaksanakan fungsi inverse untuk setiap balasan. Setiap router yang terletak di antara dua endpoints ini dapat melakukan transformasi dari paket. DNAT umumnya digunakan untuk mempublikasikan layanan di jaringan pribadi yang dapat diakses publik pada alamat IP.

Aplikasi terpengaruh oleh NAT
Beberapa aplikasi Layer protokol (seperti FTP dan SIP) mengirim eksplisit alamat dalam jaringan mereka aplikasi data. FTP dalam mode aktif, misalnya, menggunakan sambungan terpisah untuk mengontrol lalu lintas (perintah) dan untuk lalu lintas data (isi file). Bila meminta transfer file, host membuat permintaan mengidentifikasi data yang sesuai dengan koneksi jaringan lapisan dan transportasi lapisan alamat. Jika tuan rumah membuat permintaan sederhana yang terletak di belakang firewall NAT, menerjemahkan alamat IP dan nomor port TCP atau membuat informasi yang diterima oleh server yang tidak valid.

The Session Initiation Protocol (SIP) mengatur suara melalui IP (VoIP) komunikasi dan menderita masalah yang sama. SIP dapat menggunakan beberapa port untuk mengatur sambungan dan mengirimkan suara melalui streaming RTP. Alamat IP dan nomor port yang di encoded payload data dan harus diketahui sebelum traversal dari NATs. Tanpa teknik khusus, seperti pingsan, perilaku yang tidak terduga NAT dan komunikasi Mei gagal. Aplikasi Layer Gateway (ALG) perangkat lunak atau perangkat keras Mei benar masalah ini. ALG modul perangkat lunak yang berjalan pada sebuah firewall NAT pembaruan perangkatapapun payload data yang dilakukan oleh salah alamat translation. ALGs jelas perlu memahami tinggi-lapisan protokol yang mereka butuhkan untuk memperbaiki, maka setiap protokol dengan masalah ini memerlukan ALG terpisah. Lain kemungkinan solusi untuk masalah ini adalah dengan menggunakan NAT traversal teknik menggunakan protokol seperti pingsan atau ICE atau kepemilikan pendekatan dalam sesi perbatasan controller. NAT traversal dapat di kedua-TCP dan UDP berbasis aplikasi, tetapi dengan UDP berbasis teknik yang sederhana, lebih luas dipahami, dan lebih kompatibel dengan legacy NATs. Dalam kedua kasus, tingginya tingkat protokol harus dirancang dengan NAT traversal diketahui, dan tidak bekerja terpercaya di setangkup NATs atau buruk-behaved legacy NATs.

Kemungkinan lainnya adalah UPnP (Universal Plug and Play) atau Bonjour (NAT-PMP), tapi ini memerlukan kerjasama dari perangkat NAT. Paling tradisional klien-server protokol (FTP sebagai pengecualian utama), namun tidak mengirimkan informasi kontak lapisan 3 dan karenanya tidak memerlukan perawatan khusus oleh NATs. Sebenarnya, menghindari komplikasi NAT adalah suatu kebutuhan praktis saat merancang baru-lapisan protokol yang lebih tinggi hari ini.

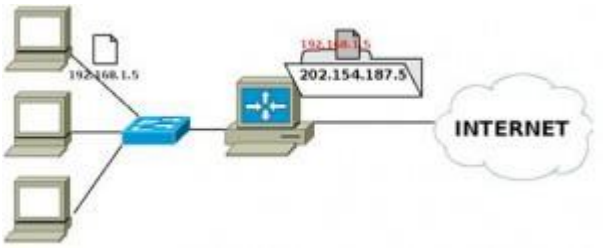
NATs juga dapat menimbulkan masalah di mana IPsec enkripsi dan diterapkan dalam kasus di mana beberapa perangkat seperti SIP telepon berada di belakang NAT. Telepon yang mengenkripsi signaling mereka dengan IPsec encapsulate pelabuhan IPsec informasi di dalam paket yang berarti bahwa NA (P) T perangkat tidak dapat mengakses dan menterjemahkan pelabuhan. Dalam kasus ini, yang NA (P) T kembali ke perangkat sederhana NAT operasi. Ini berarti bahwa semua lalu lintas kembali ke NAT akan dipetakan ke salah satu klien menyebabkan layanan gagal. Ada beberapa solusi untuk masalah ini, satu adalah dengan menggunakan TLS yang beroperasi di tingkat 4 dalam OSI Reference Model dan karenanya tidak masker nomor port, atau Encapsulate yang IPsec dalam UDP – yang kedua adalah solusi yang dipilih oleh TISPAN aman untuk mencapai NAT traversal.

Kerentanan DNS protokol yang diumumkan oleh Dan Kaminsky pada 8 Juli 2008 adalah tidak langsung dipengaruhi oleh NAT port pemetaan. Untuk menghindari server DNS cache poisoning, sangat tidak diinginkan untuk menterjemahkan sumber UDP port jumlah permintaan DNS keluar dari server DNS yang berada di belakang firewall yang menerapkan NAT. Kerja yang dianjurkan sekitar untuk kerentanan DNS adalah untuk membuat semua server DNS caching menggunakan randomized UDP port sumber. Jika fungsi dari NAT-randomizes yang sumber port UDP, DNS server yang akan dibuat rentan.

Cara Kerja dan Implementasi Network Address Translation (NAT)

Pada jaringan komputer, proses Network Address Translation (NAT) adalah proses penulisan ulang (masquerade) pada alamat IP asal (source) dan/atau alamat IP tujuan (destination), setelah melalui router atau firewall. NAT digunakan pada jaringan dengan workstation yang menggunakan IP Private supaya dapat terkoneksi ke Internet dengan menggunakan satu atau lebih IP Public. Ilustrasi NAT terlihat pada Gb. 1.

Gb 1. Network Address Translation



Kalo kita menginap di hotel tentunya kita akan mendapatkan nomor kamar bukan? Nah, alamat lengkap hotel dimana kita menginap disebut alamat publik, alamat yang dikenal oleh orang luar. Sedangakan nomor kamar kita adalah alamat private. Jadi misalnya kita memesan nasi padang di luar, yang akan kita sebutkan alamatnya adalah alamat lengkap hotel tersebut, bukan alamat kamar kita kan? Sedangkan kita tahu bahwa bisa jadi yang menginap di hotel itu nggak hanya kita. Jadi kepemilikan alamat hotel tersebut itulah yang disebut KTP bersama. Nah, nasi padang yang kita pesan nanti tentunya akan tiba di resepsionis, lalu nanti resepsionis akan meminta seorang OB untuk mengantarkan pesanan kita ke kamar anda. Fungsi resepsionis inilah yang kita sebut NAT, contoh lainnya, ternyata telpon kita di hotel hanya bersifat lokal, untuk dapat menghubungi orang diluar, kita harus mengontak resepsionis agar dapat menghubungkan kita dengan orang tersebut. Seperti itulah cara kerja NAT, menerjemahkan alamat private menjadi publik

Implementasi NAT

Pada mesin Linux, untuk membangun NAT dapat dilakukan dengan menggunakan iptables (Netfilter). Dimana pada iptables memiliki tabel yang mengatur NAT.

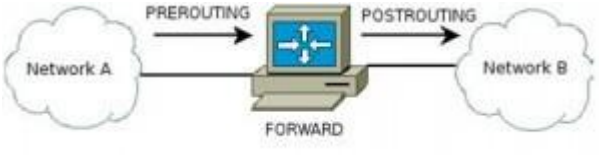
Pada tabel NAT, terdiri dari 3 chain (Gb. 2) yaitu:

– PREROUTING, digunakan untuk memilah paket yang akan diteruskan

– POSTROUTING, digunakan untuk memilah paket yang telah diteruskan

– FORWARD, digunakan untuk memilih paket yang melalui router.

Gb 2: Tabel NAT pada iptables



Proses NAT dilakukan pada data yang akan meninggalkan ROUTER. Sehingga pada iptables untuk pengolahan NAT dilakukan pada chain POSTROUTING. Rule yang diberikan kepada paket data tersebut adalah MASQUERADE.

Langkah-langkah membangun NAT dengan iptables pada Linux Router:

1. Tentukan NIC mana yang terkoneksi ke internet dan yang terkoneksi ke LAN
2. Tentukan Network Address dari LAN, misal 192.168.1.0/24
3. Menambahkan Rule di iptables

iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j MASQUERADE

Dengan menggunakan NAT ini, IP dari LAN akan dapat terkoneksi ke jaringan yang lain, tetapi tidak dapat diakses dari jaringan lain.

Manfaat

Keuntungan utama IP-masquerading NAT adalah bahwa hal itu telah menjadi solusi yang praktis mendatang kelelahan dari ruang alamat IPv4. Jaringan yang sebelumnya memerlukan Kelas B rentang IP atau blok alamat jaringan Kelas C dapat terhubung ke Internet dengan hanya satu alamat IP.

Aturan yang lebih umum adalah memiliki komputer yang membutuhkan bidirectional benar dan unfettered konektivitas routable disertakan dengan alamat IP, sementara yang memiliki komputer yang tidak menyediakan pelayanan kepada pengguna di luar keletihan jauh di belakang NAT dengan hanya beberapa alamat IP yang digunakan untuk mengaktifkan akses internet.

Beberapa juga disebut proyek keuntungan yang besar keberatan, karena penundaan perlunya penerapan IPv6, kutipan:

"… Ada kemungkinan bahwa [NAT] luas menggunakan akan menunda perlu mengaparkan IPv6. … Ini mungkin aman untuk mengatakan bahwa jaringan akan menjadi lebih makmur tanpa NAT, …"

Meskipun bukan solusi keamanan serius itu sendiri, kurangnya konektivitas penuh bidirectional dapat dipandang pada beberapa situasi sebagai fitur daripada batasan. Sebagaimana yang NAT tergantung pada mesin di jaringan lokal apapun untuk melakukan koneksi ke host pada sisi lain dari router, itu mencegah aktivitas berbahaya diprakarsai oleh host dari luar daerah yang mencapai host. Namun, manfaat yang sama dapat dicapai dengan implementasi firewall pada perangkat routing.

Kesimpulan

Jadi, bisa diambil suatu kesimpulan bahwa NAT menawarkan kecepatan dan keefektifan dalam mengamankan akses internet ke dalam bentuk jaringan privasi yang baru. Hal ini berkembang seiring dengan jumlah pengguna internet yang terus membesar. NAT juga menawarkan administrasi yang luar biasa fleksibel sehingga telah diakui oleh dunia.