Pada peremuan ini saya melampirkan sebuah video yang menjelaskan tentang proses Network Adress Translation. Proses ini berada pada di antara layer 3 dan layer 2 OSI.

Tugas: Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

Tuliskan jawaban anda pada ms word, kemudian upload pada assignment ini.

TUGAS NETWORK ACCESS

D
I
S
U
S
U
N

Oleh

NAMA : M. Iqbal Rivana

NIM : 192420057

MAGISTER TEKNIK INFORMATIKA

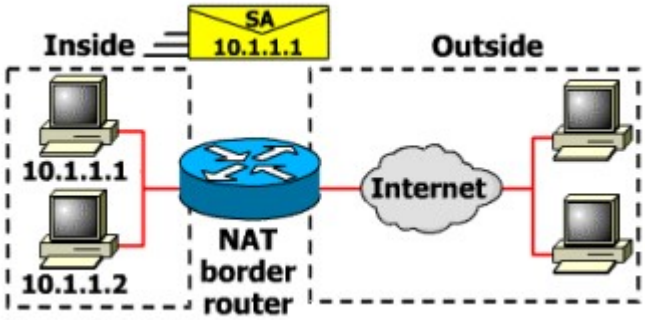
UNIVERITAS BINA DARMA

PALEMBANG

Tugas: Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

Pengertian Network Address Translation

Network Address Translation (NAT) adalah metode memetakan kembali ruang alamat IP ke yang lain dengan mengubah informasi alamat jaringan dalam header IP paket ketika sedang transit di perangkat perutean lalu lintas. Teknik ini awalnya digunakan untuk menghindari perlunya menetapkan alamat baru untuk setiap host ketika jaringan dipindahkan, atau ketika penyedia layanan Internet hulu diganti, tetapi tidak bisa merutekan ruang alamat jaringan. Ini telah menjadi alat yang populer dan penting dalam melestarikan ruang alamat global dalam menghadapi kelelahan alamat IPv4. Satu alamat IP routable-Internet dari gateway NAT dapat digunakan untuk seluruh jaringan pribadi.



Penyamaran IP adalah teknik yang menyembunyikan seluruh ruang alamat IP, biasanya terdiri dari alamat IP pribadi, di belakang satu alamat IP di tempat lain, biasanya ruang alamat publik. Alamat tersembunyi diubah menjadi alamat IP tunggal (publik) sebagai alamat sumber dari paket IP keluar sehingga mereka muncul bukan berasal dari host tersembunyi

tetapi dari perangkat perutean itu sendiri. Karena popularitas teknik ini untuk menghemat ruang alamat IPv4, istilah NAT telah menjadi hampir identik dengan IP yang menyamar.

Sebagai terjemahan alamat jaringan memodifikasi informasi alamat IP dalam paket, implementasi NAT dapat bervariasi dalam perilaku spesifik mereka dalam berbagai kasus penanganan dan pengaruhnya terhadap lalu lintas jaringan. Spesifik perilaku NAT biasanya tidak didokumentasikan oleh vendor peralatan yang mengandung implementasi NAT.

Keuntungan	Kerugian
Menghemat alamat IP legal (ditetapkan oleh NIC atau service provider)	Translasi menimbulkan delay switching.
Mengurangi terjadinya duplicate alamat jaringan IP.	Menghilangkan kemampuan 'trace' (traceability) end-to-end IP.
Meningkatkan fleksibilitas untuk koneksi ke Internet	Aplikasi tertentu tidak dapat berjalan jika menggunakan NAT.
Menghindarkan proses pengalamatan kembali (readdressing) pada saat jaringan berubah.	

NAT dasar

Jenis paling sederhana dari NAT menyediakan terjemahan alamat IP satu-ke-satu. RFC 2663 menyebut jenis NAT ini sebagai NAT dasar; itu juga disebut NAT satu-ke-satu. Dalam jenis NAT ini, hanya alamat IP, checksum header IP dan setiap checksum tingkat tinggi yang menyertakan alamat IP diubah. NAT dasar dapat digunakan untuk menghubungkan dua jaringan IP yang memiliki pengalamatan yang tidak kompatibel.

NAT satu-ke-banyak

Pemetaan alamat jaringan

Mayoritas NATs memetakan beberapa host pribadi ke satu alamat IP yang terbuka untuk umum. Dalam konfigurasi tipikal, jaringan lokal menggunakan salah satu dari subnet alamat IP pribadi yang ditunjuk (RFC 1918). Router di jaringan itu memiliki alamat pribadi di ruang

alamat itu. Router juga terhubung ke Internet dengan alamat publik yang ditetapkan oleh penyedia layanan Internet. Ketika lalu lintas lewat dari jaringan lokal ke Internet, alamat sumber di setiap paket diterjemahkan dengan cepat dari alamat pribadi ke alamat publik. Router melacak data dasar tentang setiap koneksi aktif (terutama alamat tujuan dan port). Ketika balasan kembali ke router, ia menggunakan data pelacakan koneksi yang disimpannya selama fase keluar untuk menentukan alamat pribadi di jaringan internal yang akan digunakan untuk meneruskan balasan.

Semua paket IP memiliki alamat IP sumber dan alamat IP tujuan. Biasanya paket yang lewat dari jaringan pribadi ke jaringan publik akan mengubah alamat sumbernya, sedangkan paket yang lewat dari jaringan publik kembali ke jaringan pribadi akan mengubah alamat tujuan mereka. Untuk menghindari ambiguitas dalam bagaimana balasan diterjemahkan, modifikasi lebih lanjut pada paket diperlukan. Sebagian besar lalu lintas Internet menggunakan Transmission Control Protocol (TCP) atau User Datagram Protocol (UDP). Untuk protokol-protokol ini, nomor port diubah sehingga kombinasi alamat IP dan informasi port pada paket yang dikembalikan dapat secara jelas dipetakan ke tujuan jaringan pribadi yang sesuai. RFC 2663 menggunakan istilah alamat jaringan dan terjemahan port (NAPT) untuk jenis NAT ini. Nama-nama lain termasuk terjemahan alamat port (PAT), penyamaran IP, kelebihan NAT dan banyak-ke-satu NAT. Ini adalah jenis NAT yang paling umum dan telah menjadi identik dengan istilah "NAT" dalam penggunaan umum.

Metode ini memungkinkan komunikasi melalui router hanya ketika percakapan berasal di jaringan pribadi karena transmisi awal berasal adalah apa yang menetapkan informasi yang diperlukan dalam tabel terjemahan. Peramban web di jaringan yang disamarkan dapat, misalnya, meramban situs web di luar, tetapi peramban web di luar tidak dapat meramban

situs web yang dihosting di dalam jaringan yang disamarkan. Protokol yang tidak didasarkan pada TCP dan UDP memerlukan teknik terjemahan lainnya.

Salah satu manfaat tambahan dari NAT satu-ke-banyak adalah bahwa itu adalah solusi praktis untuk kelelahan alamat IPv4. Bahkan jaringan besar dapat dihubungkan ke Internet menggunakan satu alamat IP publik.

Metode terjemahan Ada beberapa cara untuk mengimplementasikan alamat jaringan dan terjemahan port. Dalam beberapa protokol aplikasi yang menggunakan informasi alamat IP, aplikasi yang berjalan pada sebuah node dalam jaringan yang disamarkan perlu menentukan alamat eksternal NAT, yaitu alamat yang dideteksi oleh rekan-rekan komunikasinya, dan, lebih jauh lagi, seringkali perlu memeriksa dan mengkategorikan jenis pemetaan yang digunakan. Biasanya ini dilakukan karena diinginkan untuk mengatur jalur komunikasi langsung (baik untuk menghemat biaya pengambilan data melalui server atau untuk meningkatkan kinerja) antara dua klien yang keduanya berada di belakang NAT yang terpisah. Untuk tujuan ini, protokol Simple UDP over NATs (STUN) dikembangkan (RFC 3489, Maret 2003). Ini mengklasifikasikan implementasi NAT sebagai NAT kerucut penuh, (alamat) NAT kerucut terbatas, NAT kerucut port terbatas atau NAT simetris dan mengusulkan metodologi untuk menguji perangkat yang sesuai. Namun, prosedur ini sejak itu sudah tidak digunakan lagi karena status standar, karena metode ini tidak memadai untuk menilai banyak perangkat dengan benar. Metode baru telah distandarisasi dalam RFC 5389 (Oktober 2008) dan akronim STUN sekarang mewakili judul baru dari spesifikasi: Session Traversal Utilities for NAT.

en.wikipedia.org/wiki/Network_address_translation

TUGAS COMPUTER NETWORK AND COMMUNICATION

TUGAS NETWORK ACCESS LAYER

Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation

NAMA : Nanda S. Prawira
NIM : 192420056

MAGISTER TEKNIK INFORMATIKA

UNIVERITAS BINA DARMA

PALEMBANG

Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation

NAT (Network Address Translation)

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP publik (Grang and Gupta, 2013). Metode NAT banyak digunakan di seluruh dunia termasuk di Indonesia. Pada dasarnya semua jenis NAT beroperasi dengan cara client – server. Dalam hal ini, klien di zona internal yang memulai permintaan untuk memperoleh sumber daya dari server di zona internet publik (Masoud, 2013). Di sini semua klien akan mendapatkan alamat IP lokal yang diberikan oleh komputer server. Dengan mekanisme NAT terbatasnya IP publik tidak menjadi masalah. Salah satu syarat untuk menghubugkan komputer ke jaringan internet adalah dengan menggunakan IP publik. Melalui NAT memungkinkan beberapa node untuk berbagi satu atau lebih alamat IP publik. Gateway NAT berada pada batas jaringan lokal dan publik dan memodifikasi alamat IP lokal dan port dari paket yang diperuntukkan untuk jaringan publik.

Paket IP yang dibundel dengan IPSec, seperti AH dan ESP secara intrinsik dimaksudkan untuk melindungi integritas dari paket IP (termasuk sumber dan tujuan alamat) dari perubahan atau gangguan karena peran fundamental NAT gateway untuk memodifikasi alamat IP dalam header paket, IPSec, dan NAT memiliki ketidakcocokan intrinsik (Ahmad and Yaacob, 2012). NAT bekerja dengan mengalihkan suatu paket data dari suatu alamat IP ke alamat IP lainnya. Ketika suatu paket dialihkan, NAT akan mengingat dari mana asal paket dan kemana tujuan paket tersebut. Apabila paket kembali, NAT akan mengirimkannya ke alamat asal atau dengan kata lain host hanya akan menerima paket yang dikirim atau yang dimintanya sehingga komunikasi dapat berjalan dengan baik. Jaringan komputer LAN yang menggunakan NAT disebut dengan NATted Network. Sebagai contoh, di MikroTik NAT digunakan untuk komunikasi internal dan komunikasi eksternal maksudnya pengalihan data dapat dilakukan untuk paket yang berasal dari jaringan NATted (internal) ke jaringan luar eksternal atau dari jaringan luar menuju jaringan NATted. Hal tersebut sering disebut dengan komunikasi dua arah dari dan ke jaringan NATted atau internal. Untuk mengetahui mekanisme bagaimana sebuah NAT bekerja.

Dua Tipe NAT

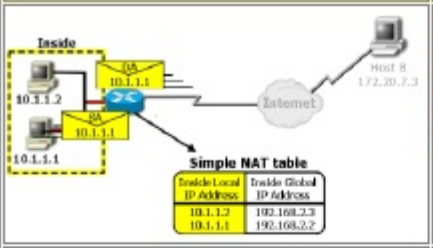
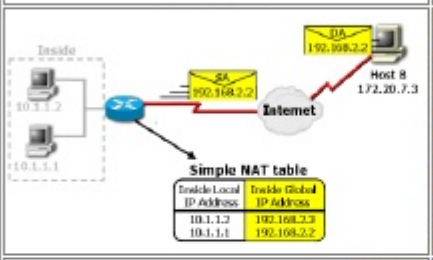
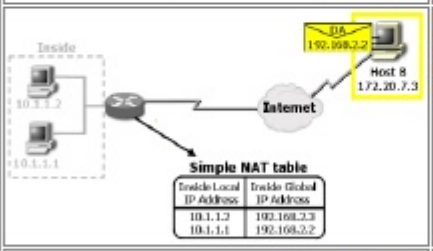
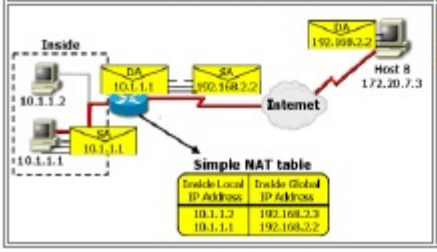
Dua tipe NAT adalah Static dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

1. **Statik**
   Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (outside) Alamat lokal dan global dipetakan satu lawan satu secara Statik.
2. **Dinamik**
   NAT dengan Pool (kelompok)
   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. Proses NAT Dinamik ini dapat memetakan bebarapa kelompok alamat lokal ke beberapa kelompok alamat global.
   NAT Overload
   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 perubahanport ke packet outbound.

Komponen-komponen NAT

NAT dapat melewatkan alamat jaringan lokal (‘private’) menuju jaringan ‘public’ seperti Internet. Alamat ‘private’ yang berada pada jaringan lokal /"inside", mengirim paket melalui router NAT, yang kemudian dirubah oleh router NAT menjadi alamat IP ISP sehingga paket tersebut dapat diteruskan melewati jaringan publik atau internet. Awalnya Fitur ini hanya tersedia pada gateway pass-through firewall saja. Tapi sekarang sudah tersedia di semua router Cisco.

Komponen Utama NAT

Gambar	Keterangan
	**Inside local IP address** – Alamat IP yang di set untuk sebuah host pada jaringan lokal (inside network). Pengalokasian alamat IP harus unik dan dalam satu subnet yang sama.
	**Inside global IP address** – Sebuah alamat IP legal (ditetapkan oleh NIC atau service provider) yang mewakili satu atau lebih alamat IP inside lokal ke dunia luar. Alamat IP ini dialokasikan dari kapasitas alamat global yang unik. Biasanya disediakan oleh Internet Service Provider (ISP).
	**Outside global IP address** – Alamat IP yang ditetapkan untuk sebuah host pada jaringan luar (outside network).
	**Simple translation** – Sebuah translasi yang memetakan satu alamat IP ke satu alamat IP lain.

Penggunaan NAT

Kapan sebaiknya NAT Digunakan?

Gunakan NAT Jika:

 Anda membutuhkan koneksi ke Internet dan hosts/komputer-komputer anda tidak mempunyai alamat IP global.

 Anda berganti ke ISP baru dan anda diharuskan menggunakan alamat IP dari ISP baru tersebut untuk jaringan anda.

NAT digunakan untuk menyelesaikan masalah pengalamatan IP

Teknologi NAT memungkinakan alamat IP lokal/’private’ terhubung ke jaringan public seperti Internet. Sebuah router NAT ditempatkan antara jaringan lokal (inside network) dan jaringan publik (outside network), dan mentranslasikan alamat lokal/internal menjadi alamat IP global yang unik sebelum mengirimkan paket ke jaringan luar seperti Internet.

Dengan NAT, jaringan internal/lokal, tidak akan terlihat oleh dunia luar/internet. IP lokal yang

cukup banyak dapat dilewatkan ke Internet hanya dengan melalui translasi ke satu IP publik/global.

Keuntungan menggunakan NAT

Jika anda harus merubah alamat IP internal anda, dikarenakan anda berganti ISP atau dua intranet digabungkan (misalnya penggabungan dua perusahaan), NAT dapat digunakan untuk mentranslasikan alamat IP yang sesuai. NAT memungkinkan anda menambah alamat IP, tanpa merubah alamat IP pada hosts atau komputer anda. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau komputer anda.

Pertimbangan Implementasi NAT

Berikut tabel keuntungan dan kerugian menggunakan NAT

Keuntungan	Kerugian
Menghemat alamat IP legal (ditetapkan oleh NIC atau service provider)	Translasi menimbulkan delay switching.
Mengurangi terjadinya duplicate alamat jaringan IP.	Menghilangkan kemampuan 'trace' (traceability) end-to-end IP.
Meningkatkan fleksibilitas untuk koneksi ke Internet	Aplikasi tertentu tidak dapat berjalan jika menggunakan NAT.
Menghindarkan proses pengalamatan kembali (readdressing) pada saat jaringan berubah.	

Nama : Rahmi

NIM : 192420046

Tugas: Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

Jawaban :

Isu penelitian (research problem) yang bisa dibahas salah satunya ***adalah*** **"Analisa Penggunaan Mekanisme Network Address Translation (NAT) untuk Menghemat Internet Protocol (IP) Address"**.

Protokol yang menjadi standar dan dipakai hampir oleh seluruh komunitas internet adalah TCP/IP *(Transmission Control Protocol/Internet Protocol)*. Agar komputer bisa berkomunikasi dengan komputer lain, maka menurut aturan TCP/IP, komputer tersebut harus memiliki suatu *address* yang unik. Alamat tersebut dinamakan IP *address.* IP *address* memiliki format sbb : *aaa.bbb.ccc.ddd.* contohnya: 167.2005.19.33.

Yang penting adalah bahwa untuk berkomunikasi di internet, komputer harus memiliki IP address yang legal. Legal dalam hal ini artinya adalah bahwa alamat tersebut dikenali oleh semua *router* di dunia dan diketahui bahwa alamat tersebut tidak ada duplikatnya di tempat lain. IP *address* legal biasanya diperoleh dengan menghubungi interNIC.

Mekanisme NAT

Sebuah paket TCP terdiri dari *header* dan data. *Header* memiliki sejumlah *field* di dalamnya, salah satu *field* yang penting disini adalah MAC *(Media Access Control) address* asal dan tujuan, IP *address* asal dan tujuan, dan nomor *port* asal dan tujuan.

Saat mesin A menghubungi mesin B, header paket berisi IP A sebagai IP *address* asal dan IP B sebagai IP *address* tujuan. *Header* ini juga berisi nomor *port* asal (biasanya dipilih oleh mesin pengirim dari sekumpulan nomor port) dan nomor port tujuan yang spesifik, misalnya port 80 (untuk *web*)

Kemudian B menerima paket pada port 80 dan memilih nomor port balasan untuk digunakan sebagai nomor port asal menggantikan port 80 tadi. Mesin B lalu membalik IP address asal dan IP A adalah IP address tujuan. Kemudian B mengirim paket itu kembali ke A. Selama session terbuka, paket data hilir, mudik menggunakan nomor port yang dipilih.

Router (yang biasa – tanpa Natd) memodifikasi field MAC address asal dan tujuan dalam header ketika me-router paket yang melewatinya. IP address, nomor port, dan nomor sequence asal dan tujuan tidak disentuh sama sekali.

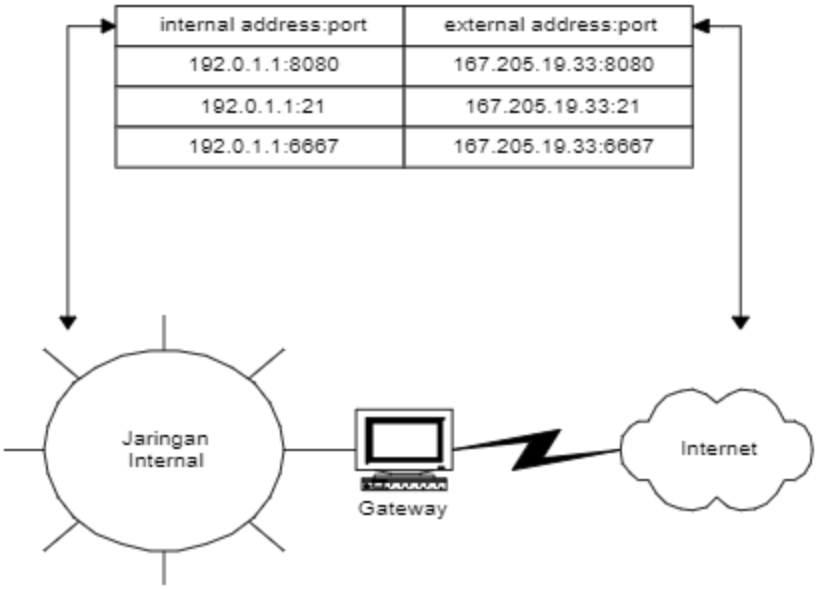
NAT juga bekerja atas dasar ini. Dimulai dengan membuat tabel translasi internal untuk smeua IP address jaringan internal yang mengirim paket melewatimya. Lalu men-set tabel nomor port yang akan digunakan oleh IP address yang valid. Ketika paket dari jaringan internal dikirim ke Natd untuk disampaikan keluar, Natd melakukan hal-hal sebagai berikut:

1. Mencatat IP address dan port asal dalam tabel translasi

2. Menggantikan nomor IP asal apker dengan nomor IP dirinya yang valid
3. Menetapkan nomor port khusus untuk paket yang dikirim keluar, memasukkannya dalam tabel translasi dan menggantikan nomor port asal tersebut dengan nomor port khusus ini.

Ketika paket balasan datang kembali, Natd mengecek nomot port tujuannya. Jika ini cocok dnegan nomor port yang khusus telah ditetapkan sebelumnya, maka dia akan melihat tabel trasnlasi dan mencari mesin mana di jaringan internal yang sesuai. Setelah ditemukan, ia akan menulis kembali port dan IP address tujuan dengan IP address dan nomor port asal yang digunakan dulu untuk memulai koneksi. Lalu mengirim paket ini ke mesin di jaringan internal yang dituju. Natd memelihara isi tabel translasi selama koneksi maish terbuka.

Gambar contoj mekanisme Natd:



Network Adress Translation

Rani Okta Felani
192420048

PROGRAM PASCASARJANA
MEGISTER TEHNIK INFORMATIKA
UNIVERSITAS BINA DARMA PALEMBANG
TAHUN 2020

Isu Penelitian Network Address Translation

NAT (Network Address Translation)

Pengertian dan jenis-jenis NAT sangat luas, tetapi intinya NAT adalah memetakan IP tertentu ke IP yang lain. Secara umum, NAT digunakan untuk mengkoneksikan IP Private ke internet melalui IP Publik. Keuntungan sistem ini adalah, hanya diperlukan sebuah/sedikit IP Publik untuk menangani banyak IP Private. Hal ini menghemat kebutuhan akan IP Publik yang jumlahnya terbatas dan harus mengeluarkan sejumlah biaya untuk mendapatkannya.

Seiring dengan meningkatnya pengguna jaringan internet, penggunaan alamat IP (*Internet Protocol*) yang terdaftar di jaringan internet juga meningkat. Untuk mengatasi permasalahan tersebut, diperlukan suatu metode yang dapat mengefisienkan penggunaan alamat IP, metode tersebut yaitu *Network Address Translation* (NAT). Metode ini telah banyak diimplementasikan pada *Internet Service Provider* (ISP), *Small Office Home Office* (SOHO) dan perusahaan-perusahaan menengah ke atas, yang memungkinkan jaringan pribadi dengan alamat IP yang tidak terdaftar di jaringan internet dapat berkomunikasi dengan jaringan internet melalui satu atau lebih alamat IP yang terdaftar di jaringan internet. *Internet Protocol Security* (IPsec) merupakan suatu set ekstensi protokol yang dikembangkan oleh *Internet Engineering Task Force* (IETF) sebagai standar mekanisme sistem keamanan pada layer IP.

Di antara NAT dan IPsec terdapat perbedaan mekanisme mendasar yang membuat perangkat IPsec di jaringan internet tidak dapat berkomunikasi dengan perangkat IPsec yang berada dibelakang perangkat NAT, hal ini dapat dilihat dari tujuan fundamental IPsec, yaitu untuk menjaga kerahasiaan data dan keutuhan data

pada layer IP, sedangkan mekanisme dari NAT justru melakukan modifikasi pada IP agar jaringan pribadi yang berada di belakangnya dapat berkomunikasi dengan jaringan publik atau internet dan begitu pula sebaliknya. Inkompatibilitas antara mekanisme kerja IPsec dan NAT telah menjadi suatu halangan dalam pengembangan implementasi IPsec sebagai standar mekanisme keamanan di layer IP, berangkat dari permasalahan tersebut, penulis tertarik untuk menganalisa mekanisme kerja dari IPsec sehingga dapat berinteraksi dengan jaringan komputer yang mengimplementasikan NAT.

ClearOS mendukung teknik NAT, baik untuk port maupun untuk ip address.

Contoh 1 : topologi dalam mode Gateway via ADSL modem (router)

Dalam contoh diatas, modem berfungsi sebagai router. Dialup dilakukan di modem (user+password dimasukkan ke modem) Jadi modem melakukan NAT dari ip publik (125.21.21.7) ke ip private (192.168.1.1). ClearOS juga melakukan NAT dari ip private modem (192.168.1.1) ke ip private LAN (172.16.5.1). Jika dialup di modem, maka IP Publik akan melekat dimodem, jika kita akses via browser, maka ip publik tersebut akan merujuk ke webconfig dari modem.

Contoh 2 : topologi dalam mode Gateway via ADSL modem (bridge):

Dalam contoh diatas, modem berfungsi sebagai bridge. Dialup dilakukan diserver ClearOS melalui opsi PPPOE (user+password dimasukkan ke server ClearOS) Dengan topologi seperti ini hanya diperlukan satu NAT, yaitu dari IP Private LAN (172.16.5.1) ke IP Publik (125.21.21.7). Jika kita akses IP publik via browser maka akan merujuk ke webconfig ClearOS.

Nama : Suwani
Nim : 192420049
MK : COMPUTER NETWORK AND COMMUNICATION

Soal : Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.
Jawaban :

NAT (Network Address Translation)

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP publik (Grang and Gupta, 2013). Metode NAT banyak digunakan di seluruh dunia termasuk di Indonesia. Pada dasarnya semua jenis NAT beroperasi dengan cara client – server. Dalam hal ini, klien di zona internal yang memulai permintaan untuk memperoleh sumber daya dari server di zona internet publik (Masoud, 2013). Di sini semua klien akan mendapatkan alamat IP lokal yang diberikan oleh komputer server. Dengan mekanisme NAT terbatasnya IP publik tidak menjadi masalah. Salah satu syarat untuk menghubugkan komputer ke jaringan internet adalah dengan menggunakan IP publik. Melalui NAT memungkinkan beberapa node untuk berbagi satu atau lebih alamat IP publik. Gateway NAT berada pada batas jaringan lokal dan publik dan memodifikasi alamat IP lokal dan port dari paket yang diperuntukkan untuk jaringan publik. Paket IP yang dibundel dengan IPSec, seperti AH dan ESP secara intrinsik dimaksudkan untuk melindungi integritas dari paket IP (termasuk sumber dan tujuan alamat) dari perubahan atau gangguan karena peran fundamental NAT gateway untuk memodifikasi alamat IP dalam header paket, IPSec, dan NAT memiliki ketidakcocokan intrinsik (Ahmad and Yaacob, 2012). NAT bekerja dengan mengalihkan suatu paket data dari suatu alamat IP ke alamat IP lainnya. Ketika suatu paket dialihkan, NAT akan mengingat dari mana asal paket dan kemana tujuan paket tersebut. Apabila paket kembali, NAT akan mengirimkannya ke alamat asal atau dengan kata lain host hanya akan menerima paket yang dikirim atau yang dimintanya sehingga komunikasi dapat berjalan dengan baik. Jaringan komputer LAN yang menggunakan NAT disebut dengan NATted Network. Sebagai contoh, di MikroTik NAT digunakan untuk komunikasi internal dan komunikasi eksternal maksudnya pengalihan data dapat dilakukan untuk paket yang berasal dari jaringan NATted (internal) ke jaringan luar eksternal atau dari jaringan luar menuju jaringan NATted. Hal tersebut sering disebut dengan komunikasi dua arah dari dan ke jaringan

NATted atau internal. Untuk mengetahui mekanisme bagaimana sebuah NAT bekerja, Gambar 1 di bawah ini merupakan contoh jaringan komputer LAN yang dihubungkan dengan gateway dan terkoneksi ke jaringan ingternet (Basuki, 2003).

Dalam FreeBSD, mekanisme *NetworkAddressTranslation* (NAT) dijalankan oleh program Natd yang bekerja sebagai *daemon*. *NetworkAddressTranslationDaemon* (Natd) menyediakan solusi untuk permasalahan penghematan ini dengan cara menyembunyikan IP *address* jaringan internal, dengan membuat paket yang di-*generate* di dalam terlihat seolah-olah dihasilkan dari mesin yang memiliki IP *address* legal. Natd memberikan konektivitas ke dunia luar tanpa harus menggunakan IP *address* legal dalam jaringan internal.

Natd menyediakan fasilitas *NetworkAddressTranslation* untuk digunakan dengan *socketdivert*. Natd mengubah semua paket yang ditujukan ke *host* lain sedemikian sehingga *source* IP *address*nya berasal dari mesin Natd. Untuk setiap paket yang diubah berdasarkan aturan ini, dibuat tabel translasi untuk mencatat transaksi ini.

Dengan NAT, aturan bahwa untuk berkomunikasi harus menggunakan IP *address* legal, dilanggar.NAT bekerja dengan jalan mengkonversikan IP-IP *address* ke satu atau lebih IP *address* lain. IP *address* yang dikonversi adalah IP *address* yang diberikan untuk tiap mesin dalam jaringan internal (bisa sembarang IP). IP *address* yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan IP *address* legal yang valid/*routable*.

Mekanisme NAT

Sebuah paket TCP terdiri dari *header* dan data. *Header* memiliki sejumlah *field* di dalamnya, salah satu *field* yang penting di sini adalah MAC (*Media Access Control*) *address* asal dan tujuan, IP *address* asal dan tujuan, dan nomor *port* asal dan tujuan.

Saat mesin A menghubungi mesin B, *header* paket berisi IP A sebagai IP *address* asal dan IP B sebagai IP *address* tujuan. *Header* ini juga berisi nomor *port* asal (biasanya dipilih oleh mesin pengirim dari sekumpulan nomor *port*) dan nomor *port* tujuan yang spesifik, misalnya *port* 80 (untuk *web*).

Kemudian B menerima paket pada *port* 80 dan memilih nomor *port* balasan untuk digunakan sebagai nomor *port* asal menggantikan *port* 80 tadi. Mesin B lalu membalik IP *address* asal & tujuan dan nomor *port* asal & tujuan dalam *header* paket. Sehingga keadaan sekarang IP B adalah IP *address* asal dan IP A adalah IP *address* tujuan. Kemudian B mengirim paket itu kembali ke A. Selama *session* terbuka, paket data hilir mudik menggunakan nomor *port* yang dipilih.

Router (yang biasa – tanpa Natd) memodifikasi *field* MAC *address* asal & tujuan dalam *header* ketika me-*route* paket yang melewatinya. IP *address*, nomor *port*, dan nomor *sequence* asal & tujuan tidak disentuh sama sekali.

NAT juga bekerja atas dasar ini. Dimulai dengan membuat tabel translasi internal untuk semua IP *address* jaringan internal yang mengirim paket melewatinya. Lalu men-*set* tabel nomor *port* yang akan digunakan oleh IP *address* yang valid. Ketika paket dari jaringan internal dikirim ke Natd untuk disampaikan keluar, Natd melakukan hal-hal sebagai berikut:

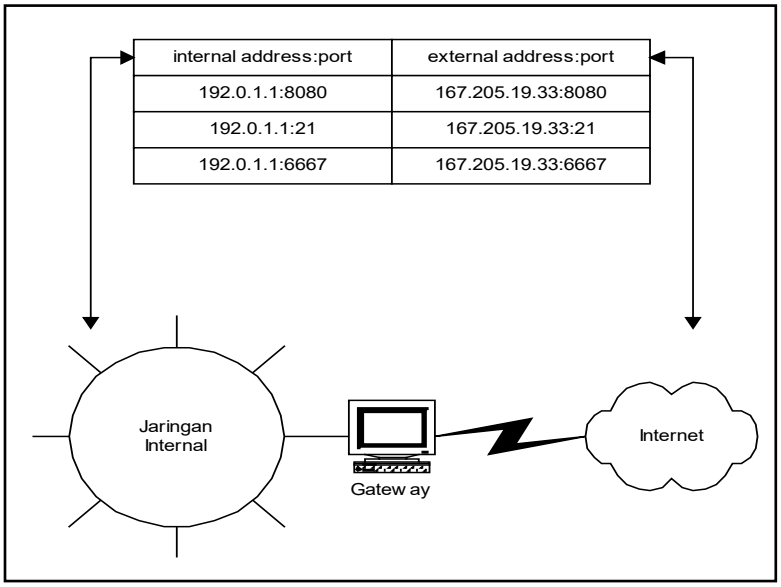
1. Mencatat IP *address* dan *port* asal dalam tabel translasi

2. Menggantikan nomor IP asal paket dengan nomor IP dirinya yang valid

3. Menetapkan nomor *port* khusus untuk paket yang dikirim keluar, memasukkannya dalam tabel translasi dan menggantikan nomor *port* asal tersebut dengan nomor *port* khusus ini.

Ketika paket balasan datang kembali, Natd mengecek nomor *port* tujuannya. Jika ini cocok dengan nomor *port* yang khusus telah ditetapkan sebelumnya, maka dia akan melihat tabel translasi dan mencari mesin mana di jaringan internal yang sesuai. Setelah ditemukan, ia akan menulis kembali nomor *port* dan IP *address* tujuan dengan IP *address* dan nomor *port* asal yang asli yang digunakan dulu untuk memulai koneksi. Lalu mengirim paket ini ke mesin di jaringan internal yang dituju. Natd memelihara isi tabel translasi selama koneksi masih terbuka.

Gambar Contoh Mekanisme Natd



Perbedaan dengan sistem *Proxy*

Hampir mirip dengan NAT, suatu jaringan kecil dengan *proxy* bisa menempatkan beberapa mesin untuk mengakses *web* dibelakang sebuah mesin yang memiliki IP *address* valid. Ini juga merupakan langkah penghematan biaya dibanding harus menyewa beberapa account dari ISP dan memasang modem & sambungan telepon pada tiap mesin.

Namun demikian, *proxy* server ini tidak sesuai untuk jaringan yang lebih besar. Bagaimanapun, menambah *hard disk* dan RAM pada server *proxy* supaya *proxy* berjalan efisien tidak selalu dapat dilakukan (karena *constraint* biaya). Lagi pula, persentase *web page* yang bisa dilayani oleh *cacheproxy* akan makin menurun sejalan dengan semakin menipisnya ruang kosong di *hard disk*, sehingga penggunaan *cacheproxy* menjadi tidak lebih baik dari pada sambungan langsung. Tambahan lagi, tiap koneksi bersamaan akan meng-*generate* proses tambahan dalam *proxy*. Tiap proses ini harus menggunakan *disk I/O channel* yang sama, dan saat *disk I/O channel* jenuh, maka terjadilah *bottle neck*.

NAT menawarkan solusi yang lebih fleksibel dan *scalable*. NAT menghilangkan keharusan mengkonfigurasi *proxy*/*sock* dalam tiap *client*. NAT lebih cepat dan mampu menangani trafik *network* untuk beribu-ribu *user* secara simultan.

Selain itu, translasi alamat yang diterapkan dalam NAT, membuat para *cracker* di Internet tidak mungkin menyerang langsung sistem-sistem di dalam jaringan internal. *Intruder* harus menyerang dan memperoleh akses ke mesin NAT dulu sebelum menyiapkan serangan ke mesin-mesin di jaringan internal. Penting di ketahui bahwa, sementara dengan NAT jaringan internal terproteksi, namun untuk masalah *security*, tetap saja diperlukan paket *filtering* dan metoda pengamanan lainnya dalam mesin NAT.

TUGAS NETWORK ACCESS

NAMA : **THEO VHALDINO**

NIM : **192420058**

ANGKATAN : **MTI22**

MAGISTER TEKNIK INFORMATIKA

UNIVERITAS BINA DARMA

PALEMBANG

Soal :

Berikan 1 contoh isu penelitian (*Research Problem*) yang bisa diangkat dari permasalahan Network Address Translation ?

Penyelesaian **:**

Isu penelitian (*Research Problem*) yang bisa dibahas salah satunya *adalah* **"ANALISA INTERKONEKSI INTERNET PROTOCOL SECURITY PADA JARINGAN KOMPUTER BERBASIS NETWORK ADDRESS TRANSLATION"** dimana dapat digambarkan sebagai berikut :

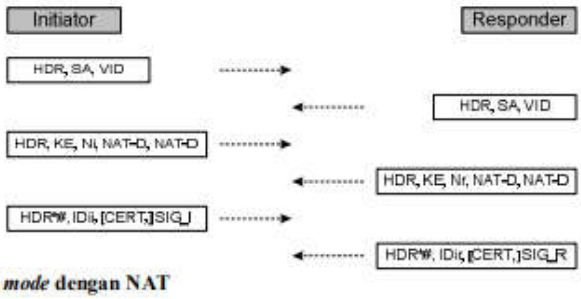
Di antara NAT dan IPsec terdapat perbedaan mekanisme mendasar yang membuat perangkat IPsec di jaringan internet tidak dapat berkomunikasi dengan perangkat IPsec yang berada dibelakang perangkat NAT, hal ini dapat dilihat dari tujuan fundamental IPsec, yaitu untuk menjaga kerahasiaan data dan keutuhan data pada layer IP, sedangkan mekanisme dari NAT justru melakukan modifikasi pada IP agar jaringan pribadi yang berada di belakangnya dapat berkomunikasi dengan jaringan publik atau internet dan begitu pula sebaliknya. Inkompatibilitas antara mekanisme kerja IPsec dan NAT telah menjadi suatu halangan dalam pengembangan implementasi IPsec sebagai standar mekanisme keamanan di layer IP.

Untuk menganalisa intekorneksi adapun Inkompabilitas dari NAT dan IPsec adalah sebagai berikut: dari Inkompatibilitas antara protokol AH dan NAT, Inkompatibilitas antara NAT dan TCP/UDP checksums, Inkompatibilitas antara identifikasi alamat IKE dan NAT, Inkompatibilitas antara IKE source port dan NA(P)T, Inkompatibilitas antara overlap inputan SPD dan NAT, serta Inkompatibilitas antara pemilihan inputan IPsec SPI dan NAT.

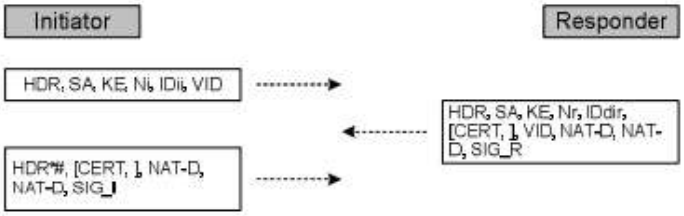
Mekanisme interkoneksi yang harus dilakukan oleh IPsec agar dapat berkomunikasi dengan perangkat yang berada di belakang NAT yaitu IKE Fase 1 :

Deteksi NAT, dimana IKE Fase 1 berlangsung,terdapat dua tipe dari deteksi NAT terjadi sebelum IKE Quick Mode (QM) dimulai, yaitu deteksi dukungan IPsec terhadap NAT dan ada atau tidaknya keberadaan NAT pada jalur komunikasi.

Di bawah ini merupakan contoh proses fase 1 main mode dan aggressive mode dengan dukungan NAT.

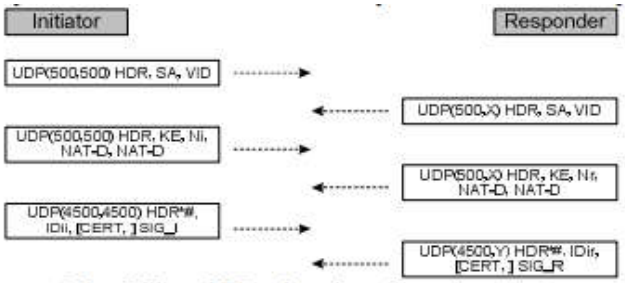


Gambar 17. Fase 1 *main mode* dengan NAT

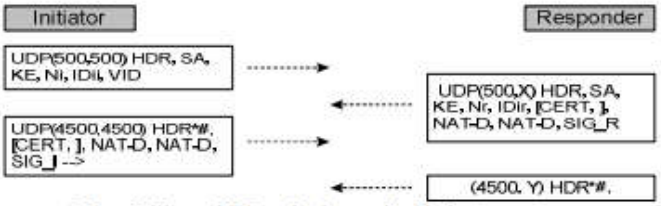


Gambar 18. Fase 1 *aggressive mode* dengan NAT

Di bawah ini contoh proses dari mekanisme perubahan port.



Gambar 19. Mekanisme perubahan IKE *port* UDP pada *main mode*

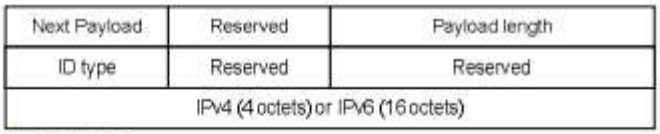


Gambar 20. Mekanisme perubahan IKE *port* UDP pada *Aggressive Mode*

Berikut ini adalah format header IKE *port* 4500

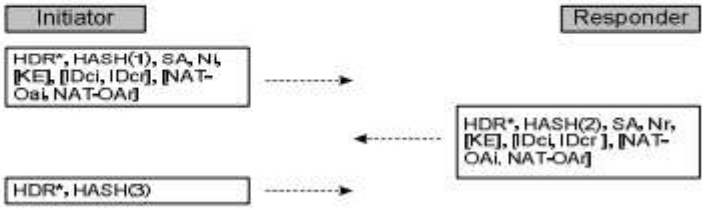
Gambar 21. Format header IKE port 4500

Di bawah ini merupakan contoh proses mekanisme quick mode dengan NAT-OA



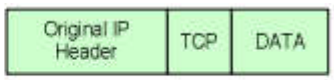
Gambar 23. Format paket NAT-OA

Di bawah ini merupakan contoh proses mekanisme *quick mode* dengan NAT-OA:

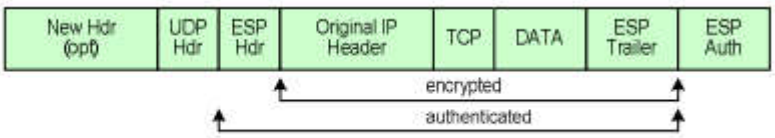


Gambar 24. Mekanisme NAT-OA *quick mode*

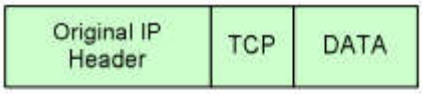
Dibawah ini proses Enkapsulasi UDP: Enkapsulasi ESP pada Transport Mode dan Tunnel Mode.



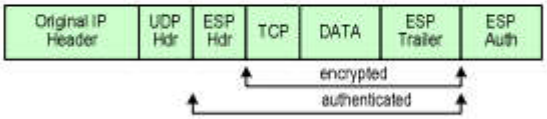
Gambar 26. IP *header*



Gambar 27. IP *header* setelah ditambah ESP dan UDP mode *tunnel*



Gambar 28. IP *header* setelah ditambah ESP dan UDP



Gambar 29. IP *header* setelah ditambah ESP dan UDP mode *transport*

Dari analisa interkoneksi IPsec pada jaringan komputer berbasis NAT yang dilakukan dapat disimpulkan bahwa :

1. IPsec dapat diimplementasikan pada jaringan berbasis NAT, dengan catatan, tidak diimplementasikannya protokol AH dan hanya mengimplementasikan protocol ESP. Karena mekanisme kerja AH mengikutsertakan IP asal dan IP tujuan dalam, NAT maupun NAT reverse bekerja dengan mengubah field address pada IP header yang akan membuat pengecekan terhadap integritas data oleh AH gagal karena data dianggap sudah tidak valid lagi. Karena protokol ESP tidak mengikutsertakan IP asal dan IP tujuan dalam integritas datanya, maka inkompatibilitas ini tidak terjadi terhadap ESP. Helmi, Analisa Interkoneksi Internet Protocol…141
2. TCP dan UDP checksums memiliki ketergantungan terhadap IP asal dan IP tujuan melalui penambahan dari pseudo header dalam perhitungannya. Sehingga ketika checksums dikalkulasi dan di cek pada sisi pengirim, hasilnya tidak sama ketika melewati perangkat NAT atau NAT reverse. IPsec ESP hanya dapat melalui NAT jika tidak melibatkan protokol TCP/UDP (IPsec pada mode tunnel atau IPsec dienkapsulasi oleh GRE), atau tidak ada pengecekan checksum, hal ini dapat dilakukan oleh UDP IPv4, karena pengecekan checksum pada UDP IPv4 bersifat opsional, sementara pada TCP IPv4, checksum diperlukan.

TUGAS UTS

TUGAS NETWORK ACCESS

NAMA : YAYAN CANDRA SUBIDIN
NIM : 192420054

MAGISTER TEKNIK INFORMATIKA

UNIVERITAS BINA DARMA

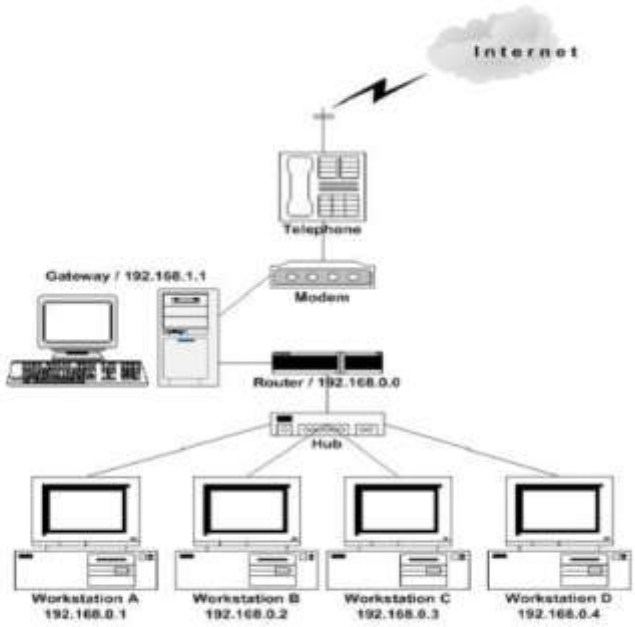
PALEMBANG

1. Tugas: Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

   Jawaban :

   Isu penelitian (research problem) yang bisa dibahas salah satunya ***adalah "Analisa Penggunaan Mekanisme Network Address Translation (NAT) untuk Menghemat Internet Protocol (IP) Address"*** dimana dapat digambarkan sebagai berikut :

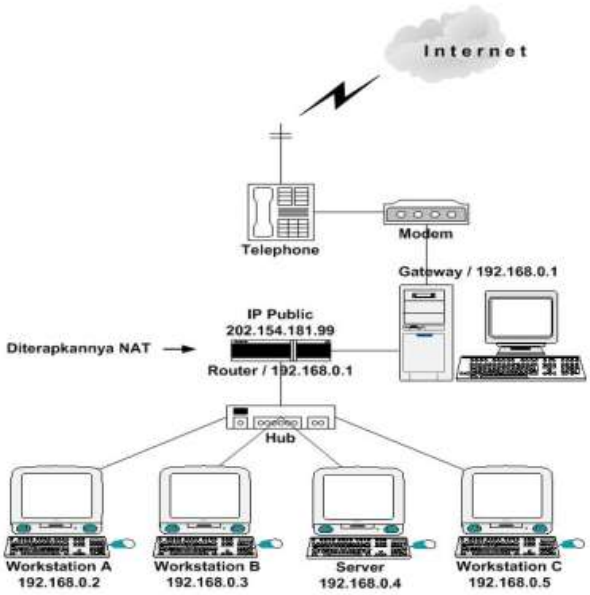
   Jenis IP address ada dua yaitu, IP public dan IP private. Dasar pertimbangan membuat IP public di kenal sebagai IP private adalah untuk memudahkan pendistribusian pendaftaran IP address. Sehingga hanya beberapa IP public yang terdaftar di Internet Service Provider (ISP) untuk pemakaian alamat lokal bisa dibuat pengalamatan IP address private sendiri.



Gambar 2. Jaringan Komputer tanpa NAT

Pada gambar 2 dapat dijelaskan bahwa untuk terkoneksi dengan internet kita perlu terhubung dengan host atau jaringan yang telah terkoneksi dengan internet gateway. Untuk memisahkan paket informasi jaringan tersebut dengan jaringan lain maka diperlukan juga router. Sehingga paket informasi yang hanya dibutuhkan untuk jaringan itu tidak akan keluar dari jaringan lokal, begitu pula sebaliknya paket informasi dari luar yang tidak ditujukan untuk komputer yang ada pada jaringan tidak akan diteruskan ke dalam jaringan lokal.

Pada gambar 3 dibawah ini adalah mengilutrasikan jaringan yang menggunakan fasilitas NAT, Jika setting IP private menggunakan IP address 192.168.0.0 maka pendistribusian IP private dari jaringan lokal adalah mulai dari 192.168.0.0 sampai dengan 192.168.0.255. Jika IP public yang dimiliki adalah 202.154.181.99 IP public ini dapat didistribusikan ke IP private melalui mekanisme NAT dengan alamat tertentu sesuai dengan setting IP private yang dibuat.



Gambar 3. Jaringan Komputer dengan NAT

Pada gambar 3 dapat disimpulkan bahwa :

1. NAT dapat digunakan jika jumlah IP yang dimiliki sedikit sedangkan komputer yang akan disambungkan ke internet cukup banyak.
2. Penggunaan mekanisme NAT dalam jaringan dapat menghemat biaya karena efisien dalam pemakaian IP public.
3. Penerapan NAT dalam jaringan dapat meningkatkan efisiensi manajemen LAN dalam internetworking

TUGAS

TUGAS NETWORK ACCESS

NAMA : AL ADRI NOFA GUSANDI
NIM : 192420053

MAGISTER TEKNIK INFORMATIKA

UNIVERITAS BINA DARMA

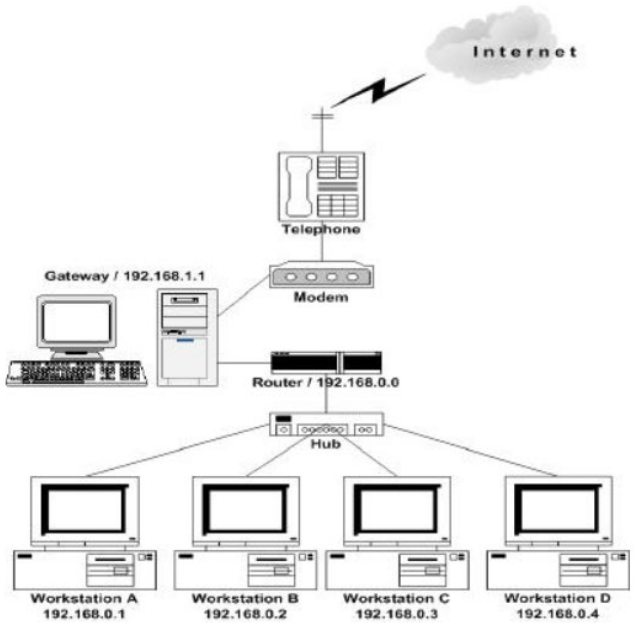
PALEMBANG

1. Tugas: Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

Jawaban :

Isu penelitian (research problem) yang bisa dibahas salah satunya **adalah "Analisa Penggunaan Mekanisme Network Address Translation (NAT) untuk Menghemat Internet Protocol (IP) Address"** dimana dapat digambarkan sebagai berikut :

Jenis IP address ada dua yaitu, IP public dan IP private. Dasar pertimbangan membuat IP public di kenal sebagai IP private adalah untuk memudahkan pendistribusian pendaftaran IP address. Sehingga hanya beberapa IP public yang terdaftar di Internet Service Provider (ISP) untuk pemakaian alamat lokal bisa dibuat pengalamatan IP address private sendiri.

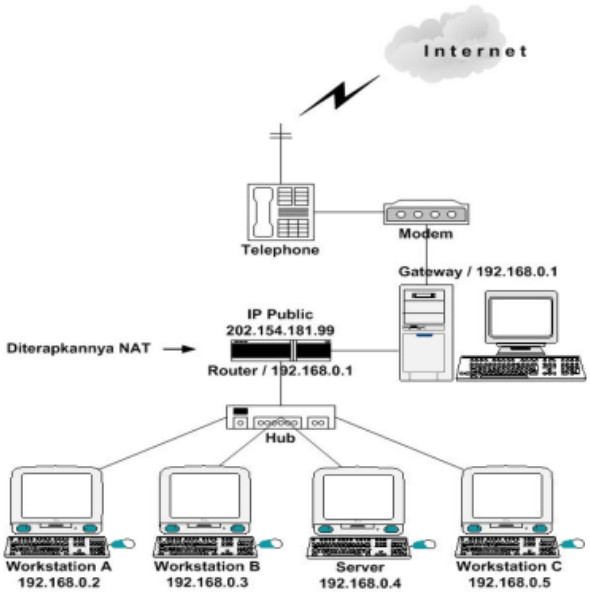


Gambar 2. Jaringan Komputer tanpa NAT

Pada gambar 2 dapat dijelaskan bahwa untuk terkoneksi dengan internet kita perlu terhubung dengan host atau jaringan yang telah terkoneksi dengan internet gateway. Untuk memisahkan paket informasi jaringan tersebut dengan jaringan lain maka diperlukan juga router. Sehingga paket informasi yang hanya dibutuhkan untuk jaringan itu tidak akan keluar dari jaringan lokal, begitu pula sebaliknya paket informasi dari luar yang tidak ditujukan untuk komputer yang ada pada jaringan tidak akan diteruskan ke dalam jaringan lokal.

Pada gambar 3 dibawah ini adalah mengilutrasikan jaringan yang menggunakan fasilitas NAT, Jika setting IP private menggunakan IP address 192.168.0.0 maka pendistribusian IP private dari jaringan lokal adalah mulai dari 192.168.0.0 sampai dengan 192.168.0.255. Jika IP public yang dimiliki adalah 202.154.181.99 IP public

ini dapat didistribusikan ke IP private melalui mekanisme NAT dengan alamat tertentu sesuai dengan setting IP private yang dibuat.



Gambar 3. Jaringan Komputer dengan NAT

Pada gambar 3 dapat disimpulkan bahwa :

1. NAT dapat digunakan jika jumlah IP yang dimiliki sedikit sedangkan komputer yang akan disambungkan ke internet cukup banyak.
2. Penggunaan mekanisme NAT dalam jaringan dapat menghemat biaya karena efisien dalam pemakaian IP public.
3. Penerapan NAT dalam jaringan dapat meningkatkan efisiensi manajemen LAN dalam internetworking

IMPLEMENTASI NETWORK ADRESS TRANSLATION

MENGGUNAKAN KERIO CONTROL VERSI 7.4.1

OLEH :

ARPA PAUZIAH

192420055

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020/2021

1. PENDAHULUAN

Pusat Penelitian (Puslit) Bioteknologi adalah satuan kerja di bawah Lembaga Ilmu Pengetahuan Indonesia (LIPI) yang merupakan lembaga penelitian di bidang bioteknologi. Sebagai lembaga yang berkecimpung dalam penelitian, kebutuhan akan data dan informasi ter-*update* adalah suatu hal yang mutlak. Hal ini penting dalam rangka menunjang pekerjaan untuk memperkaya data dan informasi terkait bidang penelitian serta mendapatkan literatur, baik buku, jurnal ilmiah, *e-book*, *e-magazine*, maupun jurnal *online*. Kebutuhan ini dapat terpenuhi, salah satunya dengan menggunakan teknologi informasi.

Kemajuan yang pesat di bidang teknologi informasi, tentunya patut disyukuri. Teknologi yang dimaksud adalah internet dan jaringan komputer global yang mendukungnya. Internet merupakan salah satu sarana yang dapat mempermudah dalam pengaksesan data dan informasi. Penyebaran data dan informasi lebih cepat melalui dunia maya, seperti *portal*, *website*, *e-journal*, *e-book*, dan jurnal *online*. Keberadaan internet mutlak adanya dan tidak bisa tergantikan. Namun, arus lalu lintas data dan internet yang lancar membutuhkan infrastruktur yang baik. Agar akses internet dapat dimanfaatkan oleh seluruh pengguna di lingkungan perusahaan atau instansi pemerintah maka diperlukan pengelolaan jaringan yang baik. Selain itu, diperlukan koneksi yang stabil juga dibutuhkan *Internet Protocol* (IP) a*ddress* agar pengguna dapat mengakses internet dengan memanfaatkan IP lokal tanpa masalah dan hambatan. Pengelolaan jaringan komputer di Puslit Bioteknologi tidak berdiri sendiri, tetapi institusi ini mendapatkan akses internet dari jaringan pusat LIPI yang dikelola oleh TGJ – LIPI. Dari Jaringan pusat LIPI membagi kepada satuan – satuan kerjanya, baik satuan kerja yang berada di Jakarta, Bandung, Cibinong, Jawa Tengah, Jawa Timur, Ambon, maupun satuan kerja lainnya. Sedangkan, Puslit Bioteknologi mendapatkan pembagian IP lokal yang beralamat di 192.168.51.1, segmen 51. IP lokal ini hanya dapat mengakomodasi pengguna yang tidak lebih dari 250 *host* komputer. Sedangkan pengguna jaringan internet di Puslit Bioteknologi tersebut samakin banyak seiring jumlah pegawai yang meningkat. Ketersediaan alamat IP terbatas sehingga jaringan LAN Puslit Bioteknologi membutuhkan pengelolaan penggunaannya sejalan dengan perkembangan jumlah *host* komputer dan alat yang terhubung ke jaringan komputer. Untuk itu, sejak beberapa tahun

terakhir, IP 192.168.51.1 sampai dengan 192.168.51.20 yang dikelola oleh Puslit Bioteknologi digunakan untuk alamat *device*, sedangkan IP 192.168.51.200 sampai dengan 192.168.51.220 digunakan sebagai alamat *web server*, *mail server*, dan sebagainya. Jadi, praktis IP yang bisa digunakan adalah antara 192.168.51.11 sampai dengan IP 192.168.51.199, sedangkan jumlah pengguna lebih dari 400 orang, ditambah lagi *device* lain, seperti *router* dan *smartphone*, dengan sisa IP tersebut sudah tidak memungkinkan lagi.

Melihat kenyataan tersebut, salah satu solusinya adalah dibutuhkan suatu mekanisme yang dapat menghemat IP tersebut. Logika sederhana, untuk penghematan IP publik adalah *share* suatu nomor IP ke beberapa *client* IP lainnya, dan mekanisme tersebut disediakan oleh NAT (Cohen, 2009). Kerio Control versi 7.4.1 menyediakan fasilitas NAT yang dapat diimplementasikan di Puslit Bioteknologi. Dengan mekanisme NAT yang disediakan Kerio Control, jaringan LAN Puslit Bioteknologi dapat terhubung ke jaringan internet walaupun hanya memiliki satu IP yang dikelola oleh LIPI.

Sebagaimana diketahui bahwa teknologi NAT saat ini secara luas digunakan, baik oleh perusahaan besar, perusahaan kecil, maupun pengguna rumahan. Hal tersebut disebabkan karena mereka tidak memiliki alamat IP yang cukup untuk memberikan satu alamat IP publik untuk setiap perangkat yang terhubung ke internet. Melalui mekanisne NAT memungkinkan beberapa komputer untuk berbagi alamat IP publik. NAT adalah solusi praktis untuk diterapkan pada jarigan yang memanfaatkan IPv4 (Zhen-hua and Zhang-yi, 2010).

Saat ini, jaringan komputer masih banyak yang menggunakan IPv4 walaupun masih sering menghadapi masalah distribusi IP yang tidak memadai. Dengan demikian, NAT merupakan solusi untuk diterapkan. Meskipun IPv6 mungkin bisa memecahkan masalah di masa depan, tetapi saat ini layanan IP masih menggunakan IPv4 sehingga masih memerlukan sistem *firewall* sederhana, seperti NAT. Selain itu, mentransfer semua komponen jaringan dari IPv4 ke IPv6 masih terhitung sangat mahal dan membutuhkan waktu yang lama untuk berkembang (Yao; Hwang; Yeh, 2014).

Tujuan utama dari implementasi NAT di Puslit Bioteknologi adalah memberikan IP yang dibutuhkan dalam jaringan lokal sehingga semua pengguna dapat memanfaatkan akses jaringan intranet, internet, dan membatasi jumlah IP yang digunakan oleh pengguna. Kajian ini

ini dibatasi pada implementasi dan konfigurasi NAT menggunakan Kerio Control versi 7.4.1 serta manfaatnya bagi pengguna di Puslit Bioteknologi.

2. TINJAUAN PUSTAKA

2.1 Internet Protocol

Internet Protocol (IP) adalah protokol yang mengatur *routing* dari pentransmisian melewati jaringan antara pengirim dan penerima. IP dapat dikatakan sebagai perantara komunikasi antar- komputer dengan menggunakan IP *address* sebagai suatu identitas dari jaringan atau komputer. IP *address* terdiri dari 32 *bit* dan terbagi menjadi dua bagian, yaitu *network* ID dan *host* ID (Rachman dan Yugianto, 2008).

IP versi 4 (IPv4) sudah ada sejak awal 1980-an dan versi ini banyak digunakan sampai saat ini. IP adalah salah satu protokol utama dalam TCP/IP. Dalam model OSI, protokol bekerja pada lapisan *network* dan fungsi utama dari protokol adalah mengidentifikasi *host* berdasarkan alamat logis mereka untuk rute data antara mereka melalui jaringan. Alamat logis dari sebuah *host* dalam jaringan adalah alamat IP dan IPv4 skema pengalamatan yang telah digunakan untuk sementara waktu sekarang dalam mengidentifikasi host dalam jaringan, sistem ini didasarkan pada 32-bit alamat logis (Babatunde dan Al-Debagy, 2014).

Beberapa aturan dasar dalam menentukan *network* ID dan *host* ID yang dapat digunakan ketika akan membangun sebuah jaringan LAN, yaitu:

a) Network ID 127.0.0.1 tidak dapat digunakan, karena merupakan *default* yang digunakan untuk keperluan menunjuk dirinya sendiri (*loop-back*);
b) *Host* ID tidak boleh di-set 1 (ex. 126.255.255.255), karena akan diartikan sebagai alamat *broadcast* (ID broadcast merupakan alamat yang mewakili seluruh anggota pada jaringan);
c) *Network* ID dan *host* ID tidak boleh sama dengan 0 (ex. 0.0.0.0), karena IP *address* dengan *host* ID 0 diartikan sebagai alamat *network* (alamat yang digunakan untuk menunjuk suatu jaringan, dan tidak menunjuk suatu *host*);
d) *Host* ID harus unik dalam suatu *network* , dan dalam suatu network tidak boleh ada dua *host* dengan *host* ID yang sama.

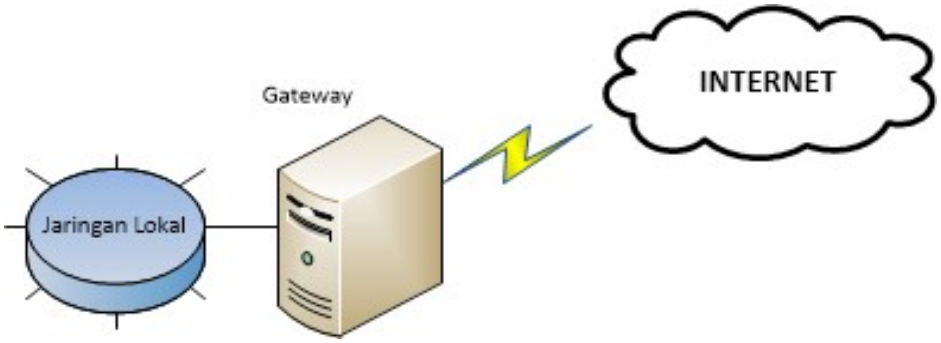
2.2 Network Address Translation

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP publik (Grang and Gupta, 2013). Metode NAT banyak digunakan di seluruh dunia termasuk di Indonesia. Pada dasarnya semua jenis NAT beroperasi dengan cara *client – server.* Dalam hal ini, klien di zona internal yang memulai permintaan untuk memperoleh sumber daya dari server di zona internet publik (Masoud, 2013). Di sini semua klien akan mendapatkan alamat IP lokal yang diberikan oleh komputer server. Dengan mekanisme NAT terbatasnya IP publik tidak menjadi masalah.

Salah satu syarat untuk menghubugkan komputer ke jaringan internet adalah dengan menggunakan IP publik. Melalui NAT memungkinkan beberapa *node* untuk berbagi satu atau lebih alamat IP publik. *Gateway* NAT berada pada batas jaringan lokal dan publik dan memodifikasi alamat IP lokal dan *port* dari paket yang diperuntukkan untuk jaringan publik. Paket IP yang dibundel dengan IPSec, seperti AH dan ESP secara intrinsik dimaksudkan untuk melindungi integritas dari paket IP (termasuk sumber dan tujuan alamat) dari perubahan atau gangguan karena peran fundamental NAT *gateway* untuk memodifikasi alamat IP dalam *header* paket, IPSec, dan NAT memiliki ketidakcocokan intrinsik (Ahmad and Yaacob, 2012).

NAT bekerja dengan mengalihkan suatu paket data dari suatu alamat IP ke alamat IP lainnya. Ketika suatu paket dialihkan, NAT akan mengingat dari mana asal paket dan kemana tujuan paket tersebut. Apabila paket kembali, NAT akan mengirimkannya ke alamat asal atau dengan kata lain *host* hanya akan menerima paket yang dikirim atau yang dimintanya sehingga komunikasi dapat berjalan dengan baik.

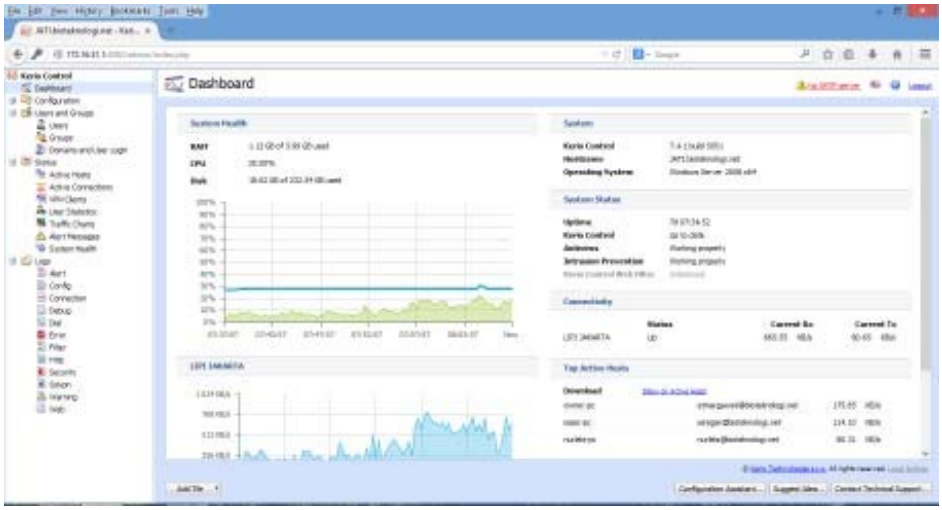
Jaringan komputer LAN yang menggunakan NAT disebut dengan *NATted Network*. Sebagai contoh, di MikroTik NAT digunakan untuk komunikasi internal dan komunikasi eksternal maksudnya pengalihan data dapat dilakukan untuk paket yang berasal dari jaringan *NATted* (internal) ke jaringan luar eksternal atau dari jaringan luar menuju jaringan *NATted*. Hal tersebut sering disebut dengan komunikasi dua arah dari dan ke jaringan *NATted* atau internal. Untuk mengetahui mekanisme bagaimana sebuah NAT bekerja, Gambar 1 di bawah ini merupakan contoh jaringan komputer LAN yang dihubungkan dengan *gateway* dan terkoneksi ke jaringan ingternet (Basuki, 2003).



Gambar 1. Mekanisme NAT

2.3 Kerio Control

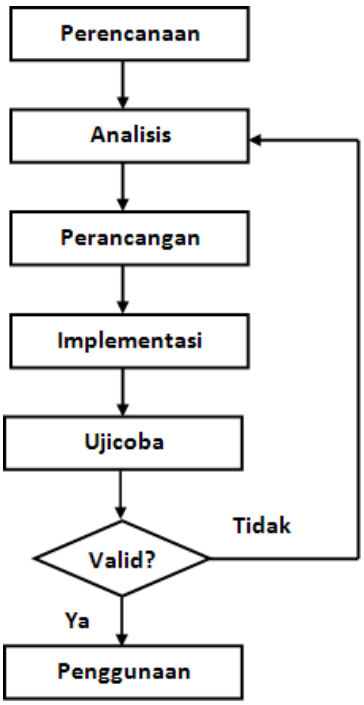
Perkembangan *WinRoute* bisa dikatakan lambat dibandingkan dengan aplikasi sejenis. Keberadaan *WinRoute* memang cukup memberikan alternatif sebagai aplikasi berkaitan dengan pemanfaatan jaringan *internet*, seperti *internet sharing*, *proxy server* NAT, dan sebagainya. Sejak versi 7, *Kerio WinRoute* namanya berubah namanya menjadi *Kerio Control* hingga saat ini. Aplikasi *Kerio Control* versi 7.4.1 yang digunakan di Puslit Bioteknologi menyediakan banyak *roles* dan *features* untuk pengaturan penggunaan jaringan internet, salah satu *features* yang digunakan adalah NAT. Dalam jaringan internet, *Kerio Control* bertindak sebagai *router* yang menerjemahkan *source* IP *address* (IP lokal) menjadi IP *address* yang berada dalam 1 *subnet* dengan *network* tujuan. Gambar 2 di bawah ini merupakan tampilan *Kerio Control* versi 7.4.1 server Pusat Bioteknologi.



Gambar 2. Tampilan *Kerio Control* versi 7.4.1 Server Puslit Bioteknologi

III. METODE

Tahapan dari siklus hidup sistem ini, meliputi tahap perencanaan, tahap analisis, tahap perancangan, tahap implementasi, dan tahap penggunaan. Tahapan-tahapan tersebut dinamakan siklus hidup pengembangan sistem atau *System Development Life Cycle* (SDLC). Penelitian ini menggunakan siklus hidup pengembangan sistem, yang merupakan serangkaian aktivitas yang dilaksanakan oleh para profesional dan pemakai sistem informasi untuk mengembangkan dan mengimplementasikan sistem informasi. Sedangkan metode yang digunakan dalam penelitian ini, mencakup langkah-langkah dan kegiatan sebagaimana terlihat pada *flowchart* Gambar 3.



Gambar 3. Pendekatan System Development Life Cycle – SDLC (Jogianto, 1989)

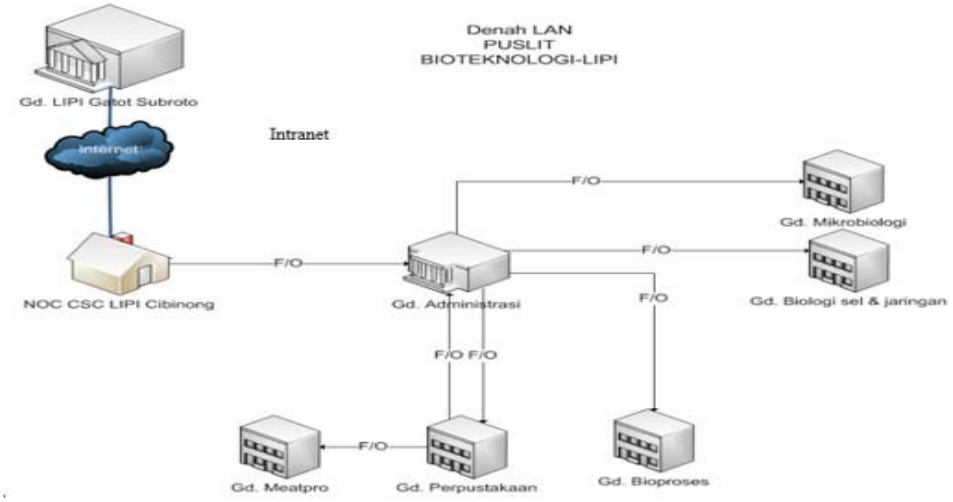
IV. HASIL DAN PEMBAHASAN

Sebelum mengimplementasikan *Kerio Control*, jaringan komputer yang ada di Puslit Bioteknologi awalnya langsung terhubung ke *Network Operation Center* (NOC) yang ada di site Cibinong. Kemudian, dari NOC terhubung ke LIPI Jakarta melalui *Fiber Optic* (F/O). Seiring dengan perkembangan TI dan pengguna internet semakin banyak,

diperlukan banyak IP untuk memenuhi kebutuhan pengguna di Puslit Bioteknologi. Dengan demikian, mulai direncanakan menggunakan *Kerio Control* sebagai *proxy server* sekaligus memanfaatkan beberapa *roles* dan *feature* yang ada di *Kerio Control* versi 7.4.1 dan *feature* NAT.

Tahapan selanjutnya adalah tahap *analisis.* Pada tahap analisis, penggunaan jaringan internet sudah menjadi kebutuhan untuk mencari data dan informasi yang berkaitan dengan penelitian, ketatausahaan, dan lain-lain. Puslit Bioteknologi mulai memanfaatkan mekanisme NAT karena dengan menggunakan IP yang ada tidak memungkinkan lagi dan tidak dapat memenuhi kebutuhan semua pengguna internet.

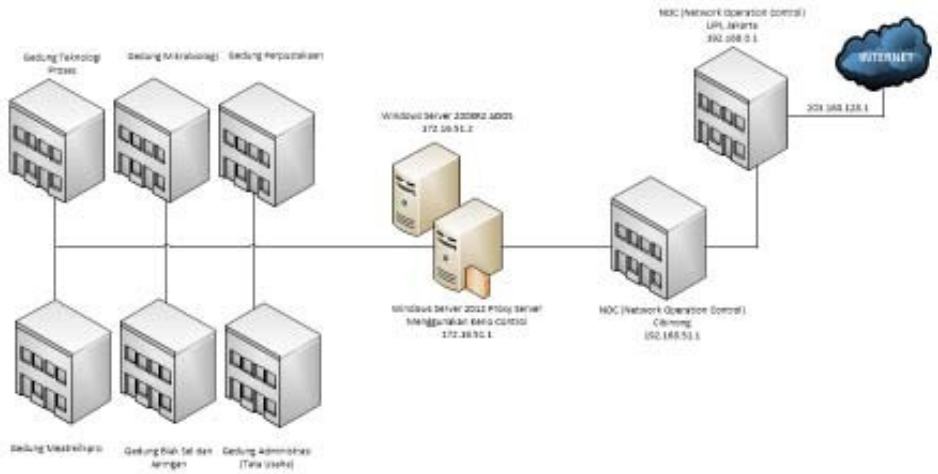
Sistem operasi yang digunakan dalam jaringan komputer (LAN) Puslit Bioteknologi adalah *Win- dows Server* 2008R2 dengan memanfaatkan *Active Diretory Domain Services* (ADDS). Dengan ADDS semua pengguna dibuat di server dan terjadi sinkronisasi antara *Server ADDS* dengan *Server Kerio Control*. Sedangkan untuk mendapatkan koneksi internet, LAN Puslit Bioteknologi harus mengakses jaringan yang ada di NOC LIPI Jakarta terlebih dahulu dengan menggunakan media F/O agar mendapatkan *IP Public*. Sedangkan topologi jaringan yang ada saat ini dijelaskan pada Gambar *Kerio Control* digunakan sebagai *proxy server* dan aplikasi *router* yang berjalan di atas sistem operasi *Windows Server* 2012 dengan *Kerio Control* versi 7.4.1 yang sudah menyediakan NAT yang dibutuhkan jaringan LAN Puslit Bioteknologi. Gambar 4 di bawah ini merupakan perancangan cara kerja NAT di Puslit Bioteknologi.



Gambar 4. Topologi jaringan Bioteknologi

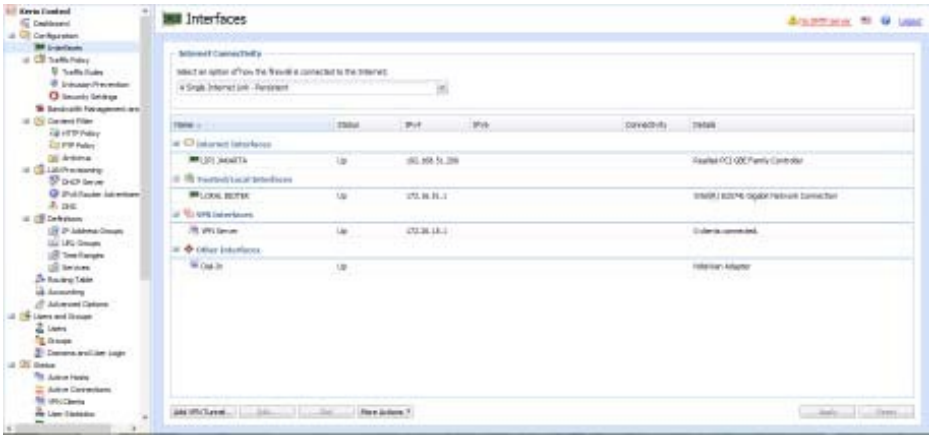
Jaringan LAN Puslit Bioteknologi terpasang di Gedung Administrasi, Gedung Mikrobiologi, Gedung Biologi Sel & Jaringan, Gedung Bioproses, Gedung Meatpro, dan Gedung Perpustakaan. Sementara itu, ruang *server* atau NOC Puslit Bioteknologi ditempatkan di salah satu ruangan Gedung Perpustakaan serta Jaringan LAN terhubung dengan Jaringan LIPI Terpadu (JALITA) LIPI Jakarta. Langkah awal menghubungkan jaringan LAN Puslit Bioteknologi adalah harus melewati *gate-way* yang dengan IP 172.16.51.1 (sekaligus sebagai *proxy server*) dan menyambungkannya dengan jaringan NOC yang ada gedung Pusinov-LIPI Cibinong. Kemudian, NOC terhubung ke Jaringan LAN LIPI Jakarta dengan menggunaan *network* 192.168.51.0 dan *gateway* 192.168.51.1. Jaringan LAN LIPI Jakarta adalah gedung yang terhubung langung dengan ISP sehingga memiliki IP publik yang dapat digunakan oleh semua jaringan yang tergabung dengan jaringan LIPI. Setelah terhubung dengan jaringan JALITA, jaringan Puslit Bioteknologi dapat mengakses *internet* dengan IP publik yang diberikan oleh *Internet Sevice Provider* (ISP). IP publik yang diberikan dapat digunakan bersama-sama dengan pengguna dari setiap satuan kerja yang ada di lingkungan LIPI. Semua pengguna yang telah memiliki akun dan terdaftar di ADDS, kemudian disinkronisasi dengan *Kerio Control* sehingga pengguna secara otomatis ketika akan masuk ke jaringan internet harus menggunaikan akun (*account*) yang dibuat di ADDS Windows Server 2008R2 atau 2012 (Whittaker, 2012).

Di ADDS, pengguna harus memasukkan akun dan *password* yang telah dibuat melalui halaman web autentifikasi untuk mengkonfirmasi akun dan *password* yang dimiliki pengguna sehingga disahkan oleh NTLM atau *login* dari *host* yang sesuai. Setelah sukses diautentifikasi, pengguna ditentukan dalam aturan NAT kemudian diizinkan untuk mengakses layanan internet lainnya. Pengguna yang tidak ditentukan dalam aturan NAT akan menjadi batasan untuk mengakses situs web atau layanan internet lainnya (Ferschmannová, 2014). Gambar 5 di bawah ini merupakan contoh alur kerja NAT.



Gambar 5. Alur cara kerja NAT

Tahapan pertama dalam implementasi adalah melakukan instalasi *Kerio Control* 7.4.1 sebagai *software* yang digunakan untuk mengkonfigurasi *proxy server* dan NAT. Selanjutnya, konfigurasi *proxy server* dan NAT dimulai dengan mengatur *interface* pada *Kerio Control*. Gambar 6 di bawah ini merupakan contoh pengaturan *interface* pada *Kerio Control.*



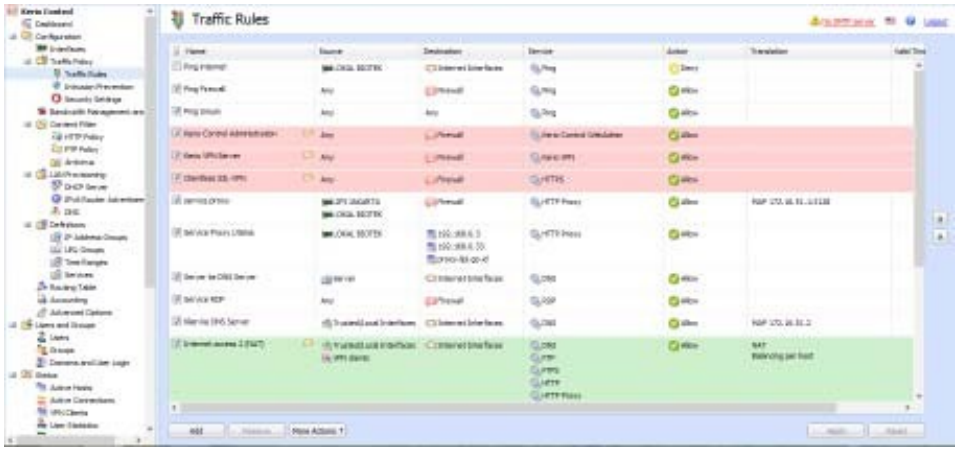
Gambar 6. Pengaturan *interface* pada *Kerio Control*

Pada komputer server yang digunakan untuk menginstalasi *Kerio Control* versi 7.4.1 dipasang dua kartu jaringan atau *Network Interface Card* (NIC) yang diperlukan pada *interface*. *Ethernet* pertama yang digunakan oleh *internet interfaces* dengan IP 192.168.51.206 telah menghubungkan LAN Puslit Bioteknologi ke NOC yang berada di

Gedung Pusinov-LIPI Cibinong. Kemudian, dari NOC - CSC (*Cibinong Science Center*) langsung terhubung ke jaringan LIPI yang ada di LIPI Jakarta. Pada *local interface* digunakan NIC kedua yang berfungsi sebagai *gateway* dengan IP 172.16.51.1 dari LAN Puslit Bioteknologi.

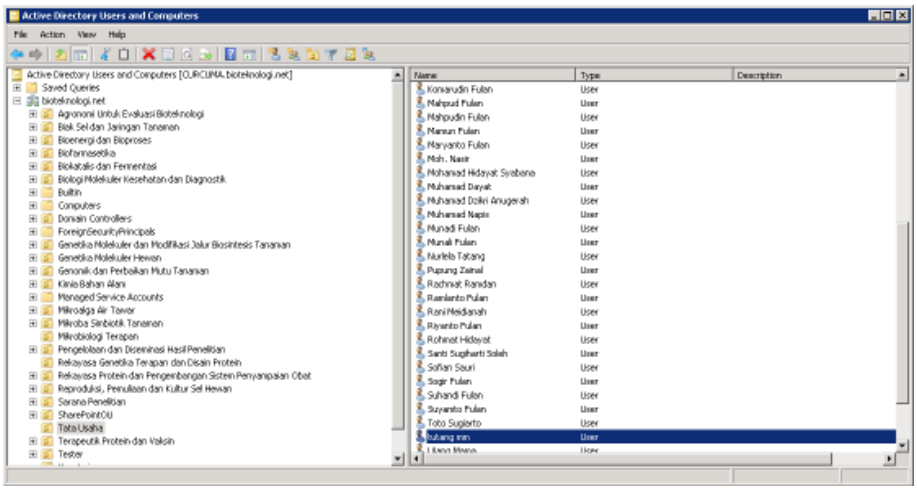
Tahapan implementasi berikutnya adalah konfigurasi pada menu *Traffic Rules*. Pada menu *Traffic Rules* didaftarkan kebijakan NAT yang digunakan. Terdapat dua *rules* untuk fasilitas NAT, yaitu:

1) *rules* pertama didaftarkan dengan nama "*Internet Access* (NAT)", *rules* ini merupakan *default* dari *Kerio Control* dan pada saat dilakukan instalasi *Kerio Control*, *rules* tersebut telah terkonfigurasi secara otomatis pada saat *software* pertama kali digunakan;
2) *rules* kedua didaftarkan dengan nama "*Internet access 2* (NAT)". Mengenai masing-masing konfigurasi *rules* pertama dan kedua ditampilkan pada Gambar 7 di bawah ini.



Gambar 7. Penerapan NAT pada menu *Traffic Rules*

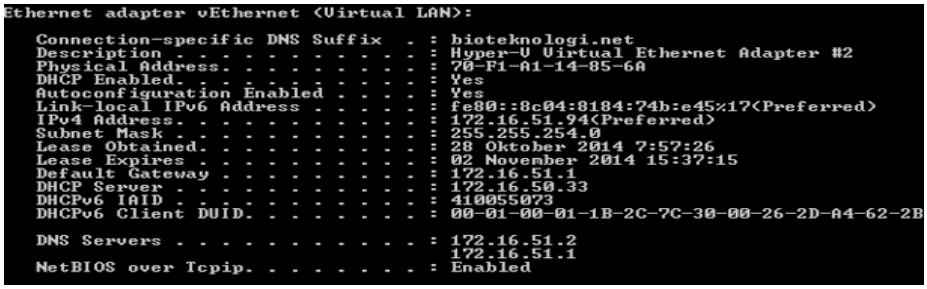
Pada *rules* pertama *source* diisi dengan *Authenticated User*. *Authenticated User* yang dimaksud adalah pengguna yang telah terdaftar ADDS *Microsoft Windows Server* 2008R2, kemudian disinkronisasi dengan *Kerio Control* versi 7.4.1. Pengguna yang telah terdaftar di *Domain Control* secara otomatis akan terhubung ke *Kerio Control* versi 7.4.1. Sementara itu, *Destination* pada *Rules* merujuk ke *Internet Interface* yang telah dikonfigurasi sebelumnya. Semua s*ervice* digunakan dalam NAT di Puslit Bioteknologi. Terdapat tiga *action* pada konfigurasi NAT ini, yaitu *Allow Deny* dan *Drop*. Pada *Rules translation* di menu *Traffic Rules* diatur oleh NAT *Balancing per host*, di sini semua *traffic* dari setiap *host* dalam jaringan LAN akan di *route* ke *internet link* yang sama.



Gambar 8. *Active Directory Users* and *Computers Windows Server* 2008R2

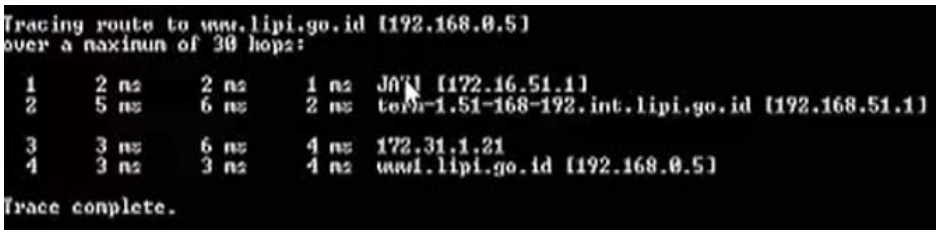
Rules kedua hampir mempunyai konfigurasi yang pertama. Hal yang membedakan adalah pada *source* diisi *Trusted/Local Interface*. User yang masuk melalui jaringan *hostspot* atau *WiFi* akan menggunakan *Rules* ini untuk mendapatkan *IP Public*. Selain *source*, hal lain yang membedakan adalah *service* yang digunakan pada *rules* kedua.

Tahap pengujian bertujuan untuk mengecek kesesuaian hasil konfigurasi dengan alur perancangan yang dibuat, pengujian dilakukan untuk memastikan LAN Puslit Bioteknologi dalam mendapatkan IP publik untuk mengakses internet. Pengujian dapat terlihat ketika melakukan *tracert* untuk menunjukkan *rute* yang dilewati paket untuk mencapai tujuan. Langkah pengujian pertama adalah melakukan *ipconfig* pada salah satu *user* LAN Puslit Bioteknologi. Hasil dari *ipconfig* ditunjukkan pada Gambar 9 dan informasi yang ditunjukkan dengan menggunakan perintah *ipconfig* tersebut, diantaranya berupa *de- fault gateway*, *DHCP Server*, dan *DNS Server.*



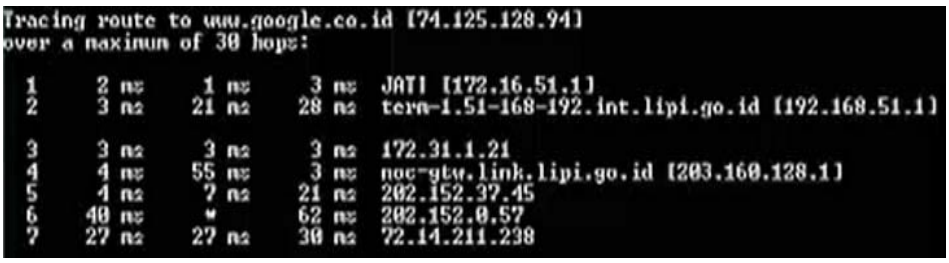
Gambar 9. Hasil *ipconfig* PC *user* di jaringan Puslit Bioteknologi

Langkah berikutnya, melakukan *tracert* pada www.lipi.co.id. Hasil *tracert* menunjukkan bahwa tujuan paket mempunyai IP 192.168.0.5, IP tujuan merupakan IP dari jaringan LIPI. Pada Gambar 10 dan Gambar 10 terlihat telah dilakukan translasi dari IP lokal di jaringan Puslit Bioteknologi dengan IP di jaringan LIPI. Paket terlebih dahulu melewati *gateway* dari jaringan lokal Puslit Bioteknologi yang memiliki IP 172.168.51.1. Setelah itu paket melewati *gateway* dari jaringan LIPI dan dilakukan translasi sehingga *user* dapat mengakses www.lipi.go.id. Hal ini sesuai dengan implementasi pada *Kerio Control* versi 7.4.1. ketika menjalankan fungsi dari NAT.



Gambar 10. Hasil *tracert* ke www.lipi.co.id

Pengujian selanjutnya adalah melakukan *tracert* ke alamat www.google.co.id menggunakan dari jaringan LAN di Puslit Bioteknologi. Melalui jaringan ini, pengguna akan mendapatkan IP publik untuk mengakses internet. Gambar 9 menjelaskan bahwa IP tujuan 74.125.128.94, paket akan diteruskan melalui *gateway* dari jaringan LAN Puslit Bioteknologi dan jaringan LIPI. Setelah itu, pengguna akan mendapatkan IP publik 203.168.128.1 agar dapat mengakses internet. Proses translasi untuk tahap ini dilakukan pada jaringan LIPI yang berhubungan langsung dengan *Internet Service Provider* (ISP). *Kerio Control* versi 7.4.1 digunakan sebagai *gateway* dari jaringan LAN Puslit Bioteknologi untuk terhubung dengan jaringan LIPI yang ada di NOC.

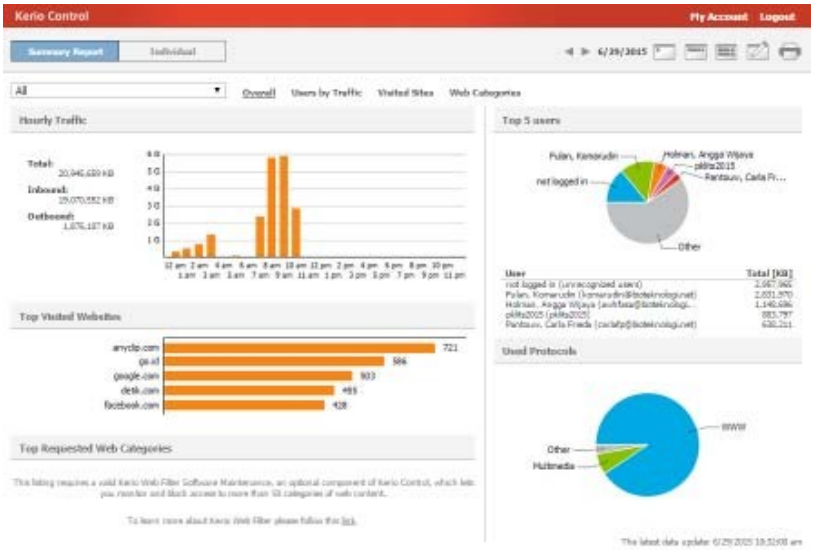


Gambar 11. Hasil *tracert* ke www.google.co.id

V. KEUNTUNGAN

Dengan diterapkannya mekanisme NAT dan *proxy* server menggunakan *Kerio Control* versi 7.4.1, jaringan LAN di Puslit Bioteknologi semakin baik dan nyaman bagi peran pengguna, khususnya peneliti. Hal tersebut menunjukkan bahwa dengan kecanggihan NAT menggunakan *Kerio Control* versi 7.4.1. memberikan banyak manfaat bagi pengguna, khususnya mengurangi komplain pengguna. Penerapan NAT dengan *Kerio Control* 7.4.1 dapat mengoptimalkan *bandwidth* jaringan. Dalam hal ini, *bandwith* jaringan internet dapat difilter dan dibatasi waktu penggunaannya, seperti penggunaan *youtube*, *download file*, *download* film, dan mendengarkan musik. Adanya pembatasan tersebut, pengguna (peneliti) ketika mencari bahan penelitian/literatur dapat lebih leluasa tanpa harus dibatasi oleh kurangnya *bandwidth*.

Namun, penggunaan situs pada waktu tertentu juga dapat menghabiskan *bandwidth* Gambar 12 memberikan contoh pada pagi hari para pengguna jaringan khususnya yang menggunakan internet ternyata lebih dominan pada situs-situs tertentu , baik oleh peneliti maupun oleh pejabat fungsional lainnya.



Gambar 12. Grafik penggunaan *Kerio Control* dan *Top Visited Website*

VI. KESIMPULAN

Keterbatasan alamat IP lokal dapat menjadi masalah besar pada sebuah lembaga atau perusahaan yang berkemban. Hal tersebut terlihat jumlah alamat IP yang terbatas tidak sebanding dengan jumlah pengguna yang semakin bertambah. Pemanfaatan metode NAT menjadi solusi terbaik untuk mengatasi hal tersebut. Pemanfaatkan *Kerio Control* versi 7.4.1 yang memiliki servis (*roles*) NAT membantu semua pengguna melalui jaringan LAN di Puslit Bioteknologi untuk mendapatkan IP publik. Mekanisme NAT dapat membuat satu IP publik yang disediakan ISP untuk LIPI, dapat digunakan oleh banyak pengguna di setiap satuan kerja di lingkungan LIPI. Dengan peningkatan kualitas akses jaringan ini, diharapkan kinerja lembaga, peneliti, dan unsur pendukungnya dapat meningkat.

DAFTAR PUSTAKA

Ahmad, Nazrul M. and Asrul H. Yaacob. 2012. "IPSec over Heterogeneous IPv4 and IPv6 Networks: Issues and Implementation". *International Journal of Computer Networks & Communications (IJCNC)*, Vol.4, No.5.

Babatunde, Olabenjo dan Omar Al-Debagy. 2014. "A Comparative Review of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)". *International Journal of Computer Trends and Technology (IJCTT)*, Vol. 13 No. 1. July.

Cohen, M.I. 2009. "Source Attribution for Network Address Translated Forensic Captures". *Digital Investigation,* 5: 138 – 145.

Ferschmannová, Vendula. 2014. "Kerio Knowledge Base, Configuring Traffic Rules". (*http:// kb.kerio.com/product/kerio-control/security/configuring-traffic-rules-1312.html#fig- ruleuseraccessex2*, diakses 17 Desember 2014).

Grang, Neha and and Anuj K.Gupta. 2013. "To Minimize the Consumption of Logical Addresses in a Network using OSPF with Overloading Technique". *Global Journal of Computer Science and Technology Network, Web & Security*, Vol. 13 Issue 11 Version 1.0.

Jogianto, H.M. 1989. *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*. Yogyakarta: Andi Offset.

Masoud, Mohammad Z. M. 2013. "Analytical Modelling of Localized P2P Streaming Systems under NAT Consideration". *International Journal of Computer Networks & Communications (IJCNC)*, Vol.5, No.3.

Rachman O dan Yugianto G. 2008. *TCP/IP dalam Dunia Informatika & Telekomunikasi*. Bandung: Informatika Bandung.

Technologies, Kerio. 2012. "Kerio Control Administrator's Guide". (*http://manuals.kerio.com/control/ adminguide/en/*, diakses 23 Desember 2014).

Whittaker, Ken. 2012. "How to Use a Windows Active Directory Group Policy Object (GPO) to Logon and logout Automatically Users from Kerio Control". (*http://kb.kerio.com/product/kerio-con- trol/microsoft-active-directory-apple-open-directory/how-to-use-a-windows-active-directory- group-policy-object-gpo-to-logon-and-logout-automatically-users-from-kerio-control- 917.html,* diakses 23 Desember 2014).

Yao, Bing-Jhih; Shaw-Hwa Hwang, Cheng-Yu Yeh. 2014. "Mathematical Model of Network Address Translation Port Mapping". *ScienceDirect, AASRI Procedia*, 8: 105 – 111.

Zhen-hua, WANG and YUAN Zhang-yi. 2010. "Research on Network Address Mapping Algorithm in IPv6 Private Network". (*http://www.sciencedirect.com/science/ journal/10058885,* diakses 17 Desember 2014).

NETWORK ADDRESS TRANSLATION

ELPINA SARI

ENTERPRISE IT INFRASTRUCTURE

192420050

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

2020

Berikan 1 contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation

Jawaban :

NAT adalah (Bahasa Inggris: Network Address Translation) 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. Sebuah perangkat NAT dapat menerjemahkan satu alamat IP "nyata" atau masyarakat ke dalam jumlah yang sangat besar dari alamat pribadi, sehingga sejumlah besar komputer dapat berbagi alamat publik tunggal. Manfaat langsung dari NAT adalah bahwa hal itu memungkinkan koneksi internet tunggal dengan satu alamat IP untuk dibagikan. IPv6. Namun, ada biaya tersembunyi: NAT istirahat protokol yang memerlukan koneksi masuk dan protokol yang membawa alamat IP di dalamnya. VoIP: aplikasi VoIP pada komputer (a "softphone") atau register telepon VoIP dengan SIP server, dan kemudian server SIP mengatakan aplikasi atau telepon ketika ada packes call.The masuk yang membawa aktual percakapan kemudian ditukar langsung antara pihak-pihak menelepon tanpa keterlibatan dari server.). NAT bekerja dengan mengalihkan suatu paket data dari suatu alamat IP ke alamat IP lainnya. Ketika suatu paket dialihkan, NAT akan mengingat dari mana asal paket dan kemana tujuan paket tersebut. Apabila paket kembali, NAT akan mengirimkannya ke alamat asal atau dengan kata lain host hanya akan menerima paket yang dikirim atau yang dimintanya sehingga komunikasi dapat berjalan dengan baik. Jaringan komputer LAN yang menggunakan NAT disebut dengan NATted Network.

Salah satu contoh permasalah dalam NAT adalah IPv6, Tetapi untuk menghubungkan, server harus dapat memberitahu setiap akhir di mana untuk mengirim paket VoIP. Ini harus menjadi nyata, alamat publik, dan bukan alamat pribadi aplikasi VoIP berpikir itu. Dan setiap akhir harus dapat menerima paket tersebut masuk, yang tidak cocok sesi keluar sebelum di NAT. Tentu saja ada cara untuk membuat karya ini, tetapi mereka memerlukan NAT untuk menyadari aplikasi dan / atau aplikasi untuk menyadari NAT. Perangkat NAT biasanya memiliki "aplikasi lapisan gateway" (algs) untuk protokol populer yang biasanya tidak bekerja melalui NAT. Misalnya, SIP ALG akan memantau lalu lintas antara aplikasi VoIP dan server SIP dan menulis ulang alamat pribadi yang melihat ada ke alamat publik NAT dan pastikan paket yang datang dari aplikasi VoIP remote disampaikan dengan benar. Atau, aplikasi dapat menggunakan protokol seperti protokol UPnP Internet Gateway atau NAT Pelabuhan Pemetaan Protocol (NAT-PMP) untuk menghubungi perangkat NAT untuk mendapatkan alamat publik dan meminta NAT untuk meneruskan paket yang masuk tertentu.

Salah satu janji IPv6 adalah bahwa jumlah hampir tak terbatas dari alamat dan baik (tapi tidak sempurna) renumbering membuat NAT tidak perlu sehingga akan sekali lagi mungkin untuk menyebarkan aplikasi baru tanpa workarounds rumit atau kegagalan acak yang meluasnya penggunaan Menyebabkan NAT di IPv4 saat ini. The Internet Engineering Task Force (IETF) secara tradisional sangat kritis terhadap NAT, tetapi meskipun begitu, ia mengembangkan teknik yang disebut Network Address Translation – Protocol Translation (NAT-PT, RFC 2766) sebagai

sarana untuk host yang menjalankan IPv6 untuk berkomunikasi dengan host yang menjalankan IPv4. Sejauh ini, cara yang biasa untuk menyebarkan IPv6 telah menjalankan IPv4 dan IPv6 side-by-side. Ini adalah mekanisme yang sangat berguna untuk server yang harus mampu berbicara dengan kedua klien IPv4 dan IPv6, tapi untuk end-user PC itu kurang masuk akal, karena ini "dual stack" mesin terus menggunakan sampai jumlah yang sama sumber daya IPv4 dari sebagai rekan-rekan mereka IPv4-only. Sayangnya, menjalankan IPv6-only berarti hanya melihat bagian dari internet yang IPv6-enabled, yang saat ini merupakan bagian yang sangat kecil. Di sinilah NAT-PT datang: menerjemahkan paket IPv6 untuk paket IPv4 sehingga IPv6-satunya host masih bisa berbicara dengan IPv4-only internet. Namun, pada bulan Juli tahun ini RFC 4966 diterbitkan yang mengatakan: Dokumen ini membahas isu-isu dengan bentuk spesifik IPv6-IPv4 mekanisme terjemahan Protokol diimplementasikan oleh Network Address Translator – Protokol Translator (NAT-PT) didefinisikan dalam RFC 2766. masalah ini cukup serius yang merekomendasikan RFC 2766 sebagai mekanisme transisi tujuan umum adalah tidak lagi diinginkan, dan dokumen ini merekomendasikan bahwa IETF harus mereklasifikasi RFC 2766 dari Usulan Standar status bersejarah.

IPv6 Keberatan ke NAT-PT mencakup semua masalah yang disebabkan oleh NAT, tapi mereka bahkan lebih buruk, karena algs tidak bisa hanya menulis ulang alamat karena alamat IPv4 dan alamat IPv6 memiliki ukuran yang berbeda. IPv6 host yang menggunakan NAT-PT harus memiliki permintaan DNS mereka melewati sebuah ALG yang menerjemahkan alamat IPv4 ke IPv6 alamat khusus yang diteruskan ke perangkat NAT-PT yang melakukan terjemahan. Ini tentu saja akan lebih menyenangkan jika ini balasan DNS dibuat khusus melarikan diri ke alam liar, di mana mereka akan membingungkan IPv6 host yang tidak menggunakan perangkat NAT-PT yang bersangkutan, dan dual stack host pada khususnya. Ada banyak masalah lain, seperti timeout, keepalives, ketidakcocokan dengan DNSSEC dan masalah dengan otentikasi dan enkripsi. Selain daftar masalah praktis, ada juga pertanyaan yang lebih mendasar: apakah kita ingin internet IPv6 untuk mewarisi pembatasan yang sama yang hadir dalam internet IPv4 saat ini? IPv6 dikembangkan sebelum NAT adalah dalam penggunaan umum, dan sejauh ini, asumsi selalu bahwa NAT di IPv6 adalah tidak perlu dan tidak diinginkan. Tetapi penggunaan NAT-PT akan cukup banyak mengimpor isu IPv4 NAT ke dunia IPv6. Di sisi lain, beberapa orang berpendapat bahwa kurangnya NAT membuat lebih sulit untuk transisi ke IPv6 karena NAT merupakan bagian integral dari cara bahwa jaringan dikerahkan. Menghilangkan alat ini akan membuat operator jaringan kurang bersedia untuk menyebarkan protokol baru. Namun, ini hanya bisa "berpikir IPv4". Untuk lebih baik atau lebih buruk, IPv6 berbeda dengan IPv4, baik sebagai hasil alami dari alamat lama dan karena IETF menggunakan kesempatan untuk mendesain ulang IP untuk membuat beberapa perbaikan yang tidak terkait dengan panjang alamat. Kecuali ISP memutuskan untuk memberikan pengguna IPv6 hanya satu alamat IPv4 seperti dengan, tidak ada akan ada kebutuhan untuk menggunakan NAT untuk sebagian besar semua konsumen. Ini berarti bahwa itu bukan mengingat bahwa algs dan workarounds lain yang membuat NAT ditoleransi akan tersedia di IPv6, bahkan jika beberapa pengguna perusahaan ingin tetap ke NAT ketika pindah ke IPv6. Jika Anda adalah seorang administrator jaringan IPv4 maka Anda tahu semua tentang Network Address Translation (NAT). NAT memungkinkan beberapa host duduk di

belakang satu perangkat gateway (yaitu firewall) untuk berbagi satu eksternal (routable publik) alamat IP. NAT menggunakan nomor port untuk memetakan traffic keluar klien ke satu alamat IP routable gateway. Dalam IPv6, NAT tidak lagi dibutuhkan dan sebenarnya tidak dianjurkan.

Penjelasan singkat tentang bagaimana IPv4 NAT bekerja. Jika 192.168.0.3 klien membuka koneksi ke sebuah situs web menggunakan port sumber 4987, lalu lintas ini pertama pergi ke firewall, karena itu adalah “router” menjembatani jaringan klien untuk semua jaringan lain. Firewall kemudian menciptakan pelabuhan baru keluar dari kolam renang yang nomor pelabuhan bebas (katakanlah 45.534) dan memberikan ke pasangan 192.168.0.3:4987. Dia kemudian mengubah alamat IP sumber dari paket ke alamat publik firewall dan port sumber ke 45534 dan menempatkan sebuah entri dalam tabel terjemahan (45.534 -> 192.168.0.3:4987). Paket tersebut kemudian diteruskan ke hop berikutnya (s) dan akhirnya ke situs klien diminta. Ketika balasan situs, paket datang kembali ke firewall untuk port tujuan 45534. firewall tampak bahwa nomor port di tabel terjemahan dan perubahan alamat IP tujuan untuk 192.168.0.3 dan port tujuan untuk 4987. Ia kemudian mengirimkan paket ke jaringan internal. Firewall terus ini untuk setiap paket sesi. Ketika sesi ditutup oleh klien (atau server), firewall melihat ini dan menghapus terjemahan (kadang-kadang ditutup oleh firewall timeout karena kurangnya lalu lintas).

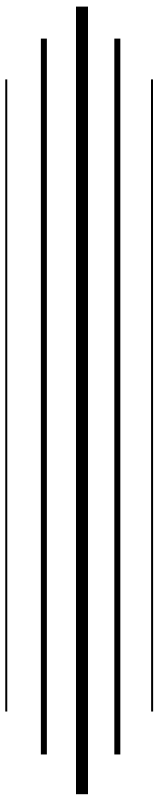
NAT secara efektif menyembunyikan jumlah host di belakang perangkat dan menyediakan satu titik masuk / keluar tunggal untuk semua klien di jaringan internal. NAT memungkinkan admin untuk mengontrol apa yang keluar atau masuk ke jaringan karena tidak ada host eksternal dapat menghubungi host internal tanpa baik lalu lintas host internal yang berasal (membuat catatan peta) atau firewall menetapkan “virtual” alamat eksternal ke alamat IP internal . Anda mungkin menggunakan NAT di rumah Anda jika Anda memiliki router nirkabel atau memiliki beberapa komputer terhubung ke Internet karena sebagian besar ISP hanya mengalokasikan satu alamat IP untuk setiap pelanggan. Router Anda meraih alamat IP yang diberikan oleh ISP Anda dan set up NAT otomatis sehingga semua komputer di rumah Anda muncul sebagai yang satu alamat ISP-ditugaskan. Router biasanya memiliki firewall stateful dibangun dan oleh default memungkinkan semua lalu lintas keluar dan tanggapan untuk lulus. Semua non-respon lalu lintas masuk diblokir (beberapa “perlindungan”).

Dalam IPv6, NAT tidak perlu (dan sebenarnya disukai) sebagai IPv6 mengembalikan benar (host-to-host) konektivitas peer-to-peer yang pada awalnya di tempat di IPv4. (Asal setiap komputer IPv4 di dunia memiliki alamat IP yang unik secara global.) Setiap komputer dapat berbicara dengan setiap komputer lain secara langsung karena setiap komputer / perangkat akan memiliki alamat IPv6 yang unik secara global. Ya, ada cukup alamat di kolam alamat untuk menghindari kelelahan di masa mendatang (dan jauh melampaui). Ingat, hanya di bagian antarmuka (rendah 64-bit) dari 128-bit alamat IPv6 ada 4,2 miliar kali ruang alamat IPv4 seluruh saat ini. Itu berarti jika ISP Anda memberikan Anda satu / 64 (yang mereka mungkin akan), Anda bisa memiliki 4,2 miliar KALI 4,2 miliar (atau 2 ^ 64) host di rumah Anda.

Bagaimana dengan “keamanan” yang NAT yang disediakan? Nah itu adalah “pergi”. KECUALI administrator jaringan masih akan memiliki satu perangkat yang rute lalu lintas antara internal (dilindungi) jaringan dan sisanya dari Internet. Pada perangkat ini (firewall), admin akan menulis aturan yang hanya memungkinkan didirikan (intern / dilindungi berasal) lalu lintas untuk memasuki jaringan. Ya, perangkat masih harus melacak sesi didirikan, tetapi tidak perlu mengutak-atik setiap paket yang keluar atau masuk ke jaringan. Juga admin dapat menulis aturan masuk untuk memungkinkan lalu lintas ke host tertentu dari internet jika diperlukan tanpa melakukan pemetaan port atau menetapkan alamat IP tambahan untuk itu.

TUGAS COMPUTER NETWORK AND COMMUNICATION

KELAS MTI 22A



DOSEN PENGASUH

Dr. Edi Surya Negara, S.Kom, M.Kom

DISUSUN OLEH:

FADEL MUHAMMAD MADJID

192420052

PROGRAM PASCA SARJANA MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

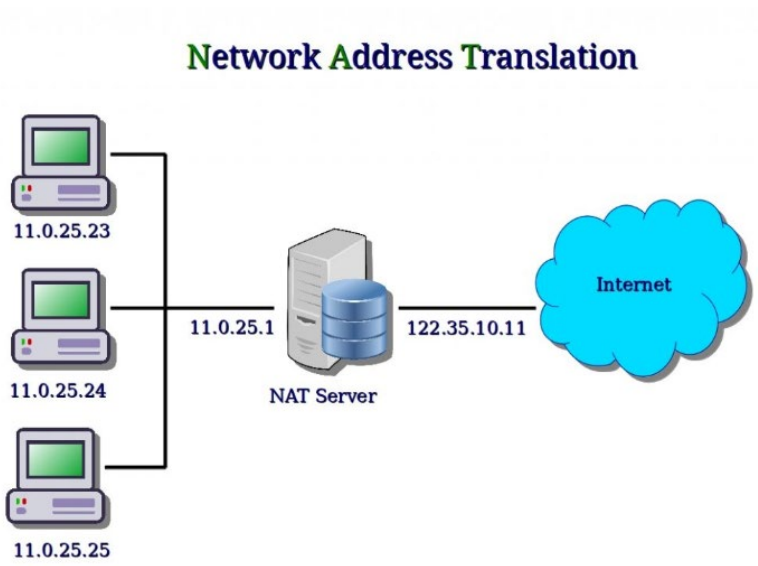
ISU PENELITIAN YANG BISA DIANGKAT DARI PERMASALAHAN NETWORK ADDRESS TRANSLATION

Dalam membangun sebuah interkoneksi jaringan LAN yang besar dibutuhkan Virtual untuk membentuk kelompok-kelompok LAN. Apalagi jika LAN sudah besar seperti di perkantoran dan kampus, masing-masing host berjarak cukup jauh. Hal ini akan akan sulit untuk membuat kelompok berdasarkan kategori tertentu jika antar host berjauhan. Akan tetapi, VLAN dapat mengatasi beberapa permasalahan yang tidak dapat diatasi oleh LAN, seperti menghubungkan 2 network berbeda dalam satu switch.

Dalam merancang jaringan computer, salah satu hal penting yang diperhatikan adalah IP Address (Alamat IP). IP Address merupakan sekumpulan biner sepanjang 32 bit yang dibagi menjadi 4 oktat di setiap oktat tersebut memeiliki panjang 8 bit. Pemberian alamat IP bisa dilakukan secara statis dan DHCP (Dynamic Host Configuration Protocol). Pemberian alamat IP secara statis dilakukan manual untuk jumlah PC yang sedikit. Jika PC yang tersedia mencapai 100 host maka akan memberikan kesulitan tersendiri bagi admin jaringan. Oleh karena itu, pemberian alamat IP dapat dilakukan dengan DHCP yaitu suatu teknik dimana PC akan meminta IP yang valid pada router dengan masuk ke dalam CLI (Command Line Interface).

Suatu jaringan memiliki arah paket yang dating dari arah yang berubah, hal ini disebabkan karena host memiliki satu alamat IP. Akan tetapi, semua orang dapat mengakses computer yang berada di belakang computer dengan memiliki alamat IP yang asli. Dalam keadaan tertentu komunikasi antar user dapat terjadi karena proses routing. Dalam proses routing komunikasi tidak dapat terjalin jika network tidak dimasukkan. Maka dalam permasalahan ini diperlukan metode agar user dapat masuk jaringan tanpa proses routing. Salah satunya dengan metode NAT statis.

Dalam perusahaan atau instansi tentunya memiliki server sebagai penyimpan atau pengolah data. Dari hal tersebut perlu adanya hak akses untuk membatasi siapa saja yang dpat mengakses server. Oleh karena itu NAT bekerja untuk mengatur hak akses yang diperbolehkan suatu IP untuk lewat. NAT merupakan pengalihan suatu alamat IP ke alamat lain, jika suatu paket dialihkan oleh NAT maka pada saat paket kembali dari tujuan akan mengingat darimana asal paket itu. Penggunaan dari NAT adalah untuk membatasi jumlah IP public baik untuk tujuan ekonomi ataupun keamanan.



NAT merupakan suatu protocol dalam suatu system jaringan yang memungkinkan suatu jaringan dengan IP yang bersifat private dimana belum terintegrasi di jaringan internet untuk mengakses jalur internet. NAT statis menggunakan table routing yang tetap, atau alokasi transaksi alamat IP ditetapkan sesuai dengan alamat asal ke alamat tujuan. Translasi terjadi ketika sebuah alamat local dipetakan ke sebuah alamat global internet. NAT secara statis akan melakukan pengambilan dan pengiriman paket data sesuai dengan aturan yang telah dilabelkan dalam sebuah NAT. Oleh karena itu, tidak ada kemungkinan pertukaran data dalam suatu alamat IP jika alamat IP belum didaftarkan dalam table NAT. Konfigurasi NAT statis juga dapat dilakukan dengan command CLI.

Dua jaringan yang belum diterapkan VLAN dalam suatu switch tidak akan terjalin dan terjadi Request Time Out (RTO) pada PC serta PC ke server. Akan tetapi jika sudah diterapkan VLAN akan terjadi Reply dari PC ke PC, namun tidak untuk PC ke server. Karena VLAN hanya dapat mengatasi PC ke PC bukan PC ke server. Oleh karena itu dapat dilakukan dengan NAT statis, dimana NAT akan menghubungkan PC ke server. NAT mampu meneruskan suatu paket IP agar dapat terhubung dalam jaringan yang berbeda. Dimana NAT dapat digunakan sebagai translator IP pada jaringan yang berbeda tanpa menggunakan proses routing.

Sumber:

Natali, J., Fajrillah, Diansyah, T.M., 2016, Implementasi Static NAT Terhadap Jaringan VLAN Menggunakan IP Dynamic Host Configuration Protocol (DHCP), Jurnal Ilmiah Informatika Vol 1 No 1.

Nama : Isti Maátun Nasichah

NPM : 192420051

Program : Magister Teknik Informatika

TUGAS

Berikan satu contoh isu penelitian (Research Problem) yang bisa diangkat dari permasalahan Network Address Translation.

Jawab :

Network Address Translation (NAT)

Network Address Translation (NAT) merupakan sebuah sistem untuk menggabungkan lebih dari satu komputer untuk dihubungkan ke dalam jaringan internet hanya dengan menggunakan sebuah alamat IP. Sehingga 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, maka pengguna tidak dapat terhubung ke internet.

Dengan NAT satu jaringan besar dapat di dipecah-pecah menjadi jaringan yang lebih kecil. Bagian-bagian kecil tersebut masing-masing akan memiliki satu alamat IP, sehingga dapat menambahkan atau mengurangi jumlah komputer tanpa mempengaruhi jaringan secara keseluruhan.

Banyak yang berpendapat bahwa NAT sebetulnya mirip dengan proxy server, namun bedanya adalah jika proxy server menyediakan mekanisme caching, tidak demikian dengan NAT. Sehingga dengan penggunaan NAT, tidak ada batasan mengenai jumlah halaman web yang dapat diakses.

Cukup banyak pengguna NAT yang memanfaatkan sistem ini, bisa jadi dikarenakan ketersediaan alamat IP yang terbatas, membutuhkan keamanan lebih, atau ada pula yang menggunakan NAT karena dinilai lebih fleksibel dalam hal

administrasi jaringan, sebab jaringan NAR didesain menyederhanakan alamat IP dan untuk melindunginya.

Dibalik semua fungsi dan kelebihan NAT, ada beberapa kekurangan yang harus dirasakan pengguna NAT, seperti mengalami *delay switching* ketika proses translasi, kehilangan kemampuan melacak IP *end to end* dan juga ada beberapa aplikasi yang menolak bekerja saat menggunakan NAT.

Voice Over Internet Protocol (VoIP)

Perkembangan teknologi informasi yang semakin pesat memberikan kemudahan bagi masyarakat untuk mengakses informasi dimanapun dan kapanpun. Voice Over Internet Protocol (VoIP) merupakan salah satu teknologi transmisi suara yang memberikan berbagai kemudahan dalam penggunaaanya dan sangat fleksibel. Teknologi ini mampu mentransmisikan paket-paket data seperti suara, video, dan paket data melalui jaringan IP untuk digunakan di berbagai tempat dan biaya yang ditawarkan juga lebih murah. Transmisi suara pada VoIP dilakukan secara digital dengan bantuan codec yang berfungsi untuk mengubah sinyal analog menjadi digital sebelum ditransmisikan. Sedangkan pada telepon analog hanya mampu melakukan transmisi suara dalam bentuk sinyal analog. Dalam implementasinya teknologi ini menggunakan jaringan yang berbeda, tidak seperti pada jaringan telepon biasa. Data-data yang dikirim dilakukan melalui jaringan IP (Internet Protocol).

VoIP Pada Jaringan Yang Menggunakan NAT

Dalam implementasinya panggilan VoIP yang dilakukan pada NAT terdapat masalah. VoIP yang diimplementasikan pada jaringan yang menggunakan NAT tidak dapat berjalan dengan baik, karena audio yang dikirim dari client yang ada dibalik jaringan NAT, tidak dapat didengar oleh client yang berada di dalam jaringan NAT. Hal ini disebabkan oleh adanya perbedaan port pada transmisi data VoIP dengan NAT. Untuk mengatasi masalah ini maka dilakukan metode tunneling.

Dengan metode ini VoIP dapat berjalan dengan baik dan masalah transmisi audio yang ada dalam jaringan NAT dapat diatasi karena semua paket data akan dilewatkan melalui jalur khusus (tunnel). Dari penelitian yang dilakukan VoIP yang diimplementasikan pada jaringan tunnel menggunakan IP tunnel untuk saling berhubungan. Sebelum data ditransmisikan ke dalam jaringan tunnel, data di

enkapsulasi menjadi IP datagram sehingga masalah yang ada dalam VoIP dengan menggunakan NAT dapat teratasi.

Struktur paket data yang ada dalam jaringan tunnel juga mengalami perubahan yaitu adanya penambahan IP header baru yang berfungsi sebagai IP tunnel dan memiliki fungsi sebagai penghubung antara vpn client satu dengan yang lain serta penambahan GRE header dan PPP header yang berfungsi dalam proses autentifikasi user vpn dan penetapan jalur data (tunnel).