ANALISIS KEAMANAN DAN PERFORMA TRANSFER DATA PADA WIDE AREA NETWORK MENGGUNAKAN GRE OVER IPSEC

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

Oleh :

Nama : Aditya Wicaksono

NIM : 06 523 257

JURUSAN TEKNIK INFORMATIKA

`FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2011

ANALISIS KEAMANAN DAN PERFORMA TRANSFER DATA PADA WIDE AREA NETWORK MENGGUNAKAN GRE OVER IPSEC

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

Oleh :
Nama : Aditya Wicaksono
NIM : 06 523 257

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA

2011

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS KEAMANAN DAN PERFORMA TRANSFER DATA PADA WIDE AREA NETWORK MENGGUNAKAN GRE OVER IPSEC

TUGAS AKHIR

Oleh :

Nama : Aditya Wicaksono

NIM : 06 523 257

Yogyakarta, Mei 2011

Pembimbing

(Syarif Hidayat, S.Kom., M.I.T.)

LEMBAR PENGESAHAN PENGUJI

ANALISIS KEAMANAN DAN PERFORMA TRANSFER DATA PADA WIDE AREA NETWORK MENGGUNAKAN GRE OVER IPSEC

TUGAS AKHIR

Oleh:

Nama : Aditya Wicaksono

NIM : 06 523 257

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, Mei 2011

Tim Penguji

Syarif Hidayat, S.Kom., M.I.T

Ketua

R. Teduh Dirgahayu, ST., M.Sc

Anggota I

Ari Sujarwo, S.Kom.

Anggota II

Mengetahui,

Ketua Jurusan Teknik Informatika

Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini

Nama : Aditya Wicaksono

NIM : 06 523 257

Tugas Akhir dengan judul :

ANALISIS KEAMANAN DAN PERFORMA TRANSFER DATA PADA WIDE AREA NETWORK MENGGUNAKAN GRE OVER IPSEC

Dengan ini saya menyatakan dengan sesungguhnya bahwa dalam tugas akhir ini tidak terdapat keseluruhan tulisan atau karya yang saya ambil dengan menyalin, meniru dalam bentuk rangkaian kalimat atau simbol atau algoritma atau program yang menunjukan gagasan atau pendapat atau pemikiran orang lain, yang saya aku seolah-olah sebagai tulisan atau karya saya sendiri.

Apabila saya melakukan hal tersebut diatas, baik sengaja atau tidak, dengan ini saya menyatakan menarik tugas akhir yang saya ajukan sebagai hasil karya saya sendiri. Bila dikemudian hari terbukti bahwa saya melakukan tindakan diatas, gelar dan ijazah yang telah diberikan oleh Universitas Islam Indonesia batal saya terima.

Yogyakarta, Mei 2011

Yang Membuat Pernyataan

(Aditya Wicaksono)

HALAMAN PERSEMBAHAN

Tugas akhir ini kupersembahkan untuk.

Allah SWT

Atas karunia dan berkah yang tidak terhingga

Papah dan Mamah

Yang selalu member dukungan atas semuanya.

Kasih sayang yang tiada batas.

Keluarga

Yang memberikan semangat dan bantuan dalam pengerjaan tugas ini

Teman-teman

Terima kasih atas bantuan , kritik, dan saran yang sangat berguna dalam membantu penyelesaian tugas ini

MOTTO

“ Ketika kita dihadapakan dengan kebuntuan, disitulah timbul jalan lain yang tidak diduga-duga arahnya”

“ Linux for Human Life, Cisco For Network”

“Konfigurasi perangkat jaringan menggunakan GUI, gak keren”

“Jika kita memiliki kawan yang pandai Ms.Word, mengapa tidak kita berdayakan?"

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Alhamdulillahi rabbil 'alamin. Segala puji bagi Allah SWT yang telah memberikan kesempatan bagi penulis untuk menyelesaikan Laporan Tugas Akhir ini. Sesungguhnya hanya atas izin dan kehendak-Nya penulis dapat menyelesaikan tugas akhir ini.

Tugas akhir ini merupakan syarat wajib di jurusan Teknik Informatika Universitas Islam Indonesia untuk memperoleh gelar sarjana. Untuk itu pada kesempatan baik ini, penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT atas segala berkah dan rahmat-Nya sehingga Tugas Akhir ini dapat diselesaikan.
2. Orang tua, kakak, dan adik atas kasih sayang, segala limpahan doa, dan dukungan
3. Yang saya hormati Bapak Ir. Gumbolo HS., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Ketua Jurusan Teknik Informatika FTI UII Bapak Yudi Prayudi S.Si.,M.Kom.
5. Bapak Syarif Hidayat S.kom M.I.T selaku dosen pembimbing tunggal dalam penyusunan Tugas Akhir ini.
6. Seluruh Dosen di Jurusan Teknik Informatika Universitas Islam Indonesia. Semoga ilmu yang telah diajarkan dapat menjadi amal, Amin.
7. Teman-teman angkatan 2006 (FIRE) di Jurusan Teknik Informatika Universitas Islam Indonesia. Rekan-rekan seperjuangan Aan khusna A S.Kom, Hendra Yunianto TS S.kom, Barly Wicaksono S.Kom, M.Yusuf Agus S, Sammy Bahaj, Ahmad Tsabit K, Prastyo Joko TK, dan banyak lagi yang tidak bisa disebutkan satu persatu.
8. P.T Prawedanet Aliansi Teknologi, Khususnya kepada bpk Yayat Soepriatna, bpk Sugeng S Rochmadi, mas Afrizal Koto, dan rekan-rekan

yang saya hormati "*Terima kasih telah membimbing dari nol sampai sekarang mengenai dunia jaringan*"

9. ID-Networkers mas Dedi Gunawan " *Terimakasih atas bimbingannya"*
10. R. Ranta Dewa yang telah mengenalkan dunia jaringan yang sebernarnya " *Terima kasih om*"
11. Specially to Aan Khusna A S.kom, Barly Wicaksono S.kom, M. Yusuf Agus S (*the ustadz*), Hendra Yunianto TS S.kom, Ahmad Tsabit K, dan Nopi Hermawan yang telah memberi peran sangat besar dalam mengerjakan TA ini " *Terima kasih kawan maaf saya menyusahkan kalian semua :D*".

Semua pihak yang tidak dapat saya sebutkan satu per satu penulis menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Untuk itu, penulis mengharapkan kritik dan saran yang bersifat membangun agar dapat berguna di kemudian hari. Penulis berharap semoga Tugas Akhir ini bermanfaat bagi semua orang, dan diri penulis sendiri. Amin.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 14 Mei 2011

Penulis

ABSTRAKSI

Teknologi jaringan komputer berkembang tanpa mengenal batasan jarak dan waktu. *Wide Area Network* (WAN) merupakan solusi untuk menghubungkan jaringan yang memiliki jarak yang saling berjauhan antara satu dan yang lainnya. Salah satu solusi yang dapat digunakan untuk mengimplementasikan WAN adalah dengan menggunakan teknologi *Virtual Private Network* (VPN)

Salah satu contoh implementasi VPN adalah dengan menggunakan *Generic Routing Encapsulation* (GRE). Penggunaan GRE dapat di kombinasikan dengan *IP Security* (IPSec) yang berguna melakukan proses enkapsulasi pada data. Penambahan header untuk enkapsulasi mungkin akan menambah beban sehingga perlu dilakukan penelitian untuk mengukur seberapa besar pengaruh implementasi GRE Over IPSec terhadap kinerja aplikasi jaringan. Beberapa aplkasi jaringan yang akan diukur dalam penelitian ini adalah *Voice Over IP* (VOIP), *File Transfer Protocol* (FTP) , dan *Internet Control Message Protocol* (ICMP).

Pengujian pada parameter VOIP akan dilakukan dengan membandingkan delay, jitter, dan paket loss baik sebelum dan sesudah pengimplementasian GRE Over IPSec dengan sample sebanyak masing-masing 10 kali. Sedangkan pada parameter FTP dan ICMP akan dibandingkan lama waktu pengiriman paket data masing-masing 6 kali dan 10 kali percobaan baik sebelum dan sesudah pengimplementasian GRE Over IPSec.

Bedasarkan pengujian menggunkan parameter diatas didapatkan kesimpulan bahwa implementasi GRE Over IPSec merupakan salah satu metode pengamanan data yang baik. Sedangkan pada perbandingan performa pada VOIP dan ICMP mengalami penurunan. Pada parameter FTP mengalami kenaikan performa setelah pengimplementasian GRE Over IPSec

Kata kunci : *Wide Area Network, Virtual Private Network*, GRE Over IPSec, Performa

TAKARIR

framework	Kerangka kerja
hash algorithms	Algoritma yang mentransformasikan beberapa karakter kedalam sebuah nilai
Private	Bersifat rahasia, tidak bisa dibuka secara umum
security gateway	Pintu keluar dan masuk yang melakukan pengamanan tertenu
Site-to-site	Tempat yang terhubung dengan tempat yang lain
Snifer	Pencuri paket
sniffing	Mencuri paket
tunnel	Terowongan penghubung

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini yang sudah sangat pesat membuat tidak ada lagi batasan jarak dan waktu, dengan semakin menghilangnya batasan geografis ini. Jaringan komputer menjadi solusi untuk memecahkan berbagai masalah yang terkait dengan batasan jarak dan waktu. Salah satunya adalah Jaringan Komputer Skala Luas atau yang biasa dikenal dengan *Wide Area Network* (WAN). WAN dapat menghubungkan antar wilayah, kota, atau negara. Dengan adanya WAN proses transfer data menjadi lebih mudah karena setiap jaringan lokal saling terhubung dengan jaringan yang lainnya.

Transfer data merupakan suatu cara berkomunikasi antara satu komputer dengan komputer yang lain dalam satu jaringan atau dengan jaringan yang lain. Komunikasi data tersebut dapat berupa saling tukar menukar informasi berupa *file* atau apapun. Proses transfer data yang melewati WAN membutuhkan keamanan dalam pengirimannya, karena WAN yang menggunakan media Internet rawan akan pencurian data tersebut.Solusi untuk mengatasi pencurian data dengan menggunakan *Virtual Private Network* (VPN) .

Virtual Private Network (VPN) merupakan sebuah metode keamanan pada transfer data yang menggunakan jaringan publik dengan cara membuat jaringan khusus secara virtual. VPN berkerja menggunakan sistem *tunneling* dan prosedur keamanan sebagai jaminan bahwa tidak ada pencurian data. Salah satu sistem tunneling yang bisa digunakan adalah *Generic Routing Encapsulation* (GRE) .

Generic Routing Encapsulation (GRE) adalah suatu protokol enkapsulasi yang dapat dilewati semua paket data dengan cara membentuk tunnel diatas jaringan publik, yang dapat menghubungkan 2 atau lebih jaringan. GRE dapat dikombinasikan dengan *IP Security* (IPSec) yang merupakan protokol yang digunakan untuk mengamankan pengiriman data dalam suatu jaringan berbasis TCP/IP. IPSec berfungsi untuk memproteksi satu atau lebih path antara sepasang host, antara sepasang *security gateway*, atau antara *security gateway* dengan host.

Penggunaan GRE over IPSec pada sistem keamanan mungkin menurunkan performa dari jaringan, hal ini dikarenakan semakin kecil ukuran isi paket data yang dapat dilewatkan dalam jaringan sehingga waktu yang diperlukan untuk mengirimkan data semakin lama. Dengan adanya hal itu maka diperlukan sebah penelitian yang membahas tentang penurunan performa jaringan yang disebabkan implementasi dari VPN dengan menggunakan GRE over IPSec menggunakan aplikasi *Voice Over IP* (VOIP), *File Transfer Protocol* (FTP), dan *Internet Control Message Protocol* (ICMP). Penggunaan aplikasi VOIP dapat mewakili pengujian protokol UDP dalam pengiriman data, pada aplikasi FTP dapat mewakili protokol TCP, dan sedangkan penggunaan aplikasi ICMP dapat mewakili proses pengecekan keadaan suatu host atau jaringan.

.

1.2 Rumusan Masalah

Dari latar belakang di atas, rumusan masalah yang dapat dikemukakan adalah bagaimana cara mengilmplematasikan sebuah topologi jaringan menggunakan teknologi GRE Over IPSec sehingga dapat dibuktikan keamanan, performa aplikasi jaringan. Aplikasi jaringan yang digunakan adalah *Voice Over IP* (VOIP), *File Transfer Protocol* (FTP), dan *Internet Control Message Protocol* (ICMP).

1.3 Batasan Masalah

Adapun batasan masalah dari tugas akhir ini adalah:

1. Implementasi VPN menggunakan IPSec dan *tunneling* menggunakan GRE.
2. aplikasi yang digunakan untuk mengukur perfoma jaringan adalah aplikasi *Voice Over IP* (VOIP), *File Transfer Protocol* (FTP), dan *Internet Control Message Protocol* (ICMP)..
3. Melakukan analisis perbedaan pada paket data baik menggunakan GRE Over IPSec maupun tidak.
4. Tidak membahas enkripsi yang digunakan.

1.4 Manfaat Penelitian

Adapun manfaat dari tugas akhir ini adalah:

1. Menjelaskan pentingnya faktor keamanan dalam proses pengiriman data.
2. Memberikan alternatif dan pengetahuan bagaimana implementasi GRE Over IPSec sebagai metode enkripsi untuk keamanan komunikasi data.
3. Menunjukkan perbaedaan performa sebelum dan sesudah menggunakan protokol GRE Over IPSec.

1.5 Metodologi Penelitian

Untuk memenuhi tujuan yang akan dicapai melalui penulisan skripsi ini, maka ada beberapa metode yang akan digunakan, yaitu:

1. Studi literatur dari buku – buku, makalah, ataupun manual – manual dan berbagai sumber online lainnya.
2. Implementasi VPN dengan protokol GRE Over IPSec dalam suatu jaringan.
3. Melakukan pengujian guna menunjukkan perbandingan performa pengiriman paket data antara sebelum dan sesudah mengunakan GRE Over IPSec dengan paramater VOIP, FTP, dan ICMP.
4. Melakukan analisis perbedaan hasil dari perbandingan tersebut.

1.6 Sistematika Penelitian

Sistematika penulisan yang digunakan adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas landasan teori dan mengenai konsep dasar WAN, VPN, GRE, IPSec, VOIP, FTP, dan ICMP.

BAB III METODOLOGI

Berisi analisis sistem dan konfigurasi yang membahas mengenai kebutuhuan perangkat keras, perangkat lunak, arsitektur sistem dan konfigurasi.

BAB IV HASIL DAN PEMBAHASAN

Berisi pengujian terhadap hasil implemenasi yang menitikberatkan pada tingkat keamanan sistem, performa dan pembahasan terhadap hasil yang didapatkan.

BAB V PENUTUP

Berisi tentang kesimpulan dan saran.

BAB II
LANDASAN TEORI

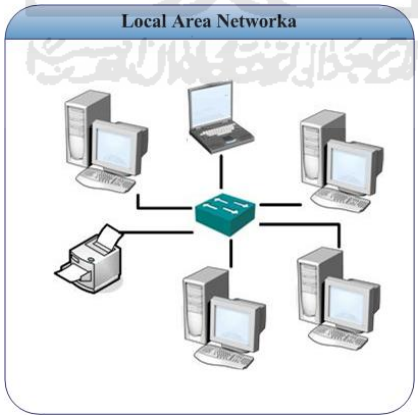
2.1 Skalabilitas Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer, software dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah :

1. Membagi sumber daya: contohnya berbagi pemakaian printer, CPU, memori, harddisk.
2. Komunikasi: contohnya surat elektronik, *instant messaging*, *chatting* Akses informasi: contohnya *web browsing.*

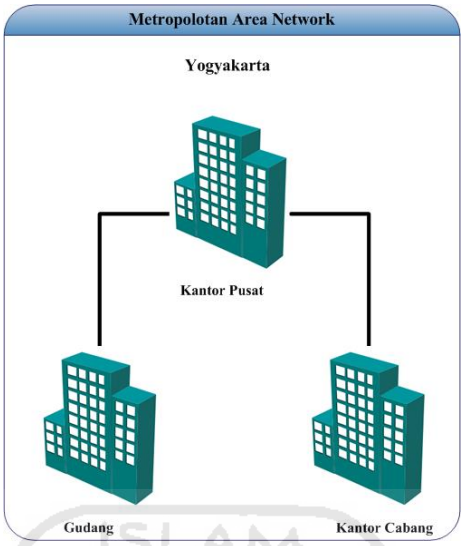
Skalabilitas jaringan dibagi menjadi 3 bagian yaitu: *Local Area Network* (LAN) *Metropolitan Area Network* (MAN) dan *Wide Area Network* (WAN) Ketiganya akan dijelaskan dibawah ini

Local Area Network (LAN) adalah gabungan dari beberapa komputer yang saling terhubung dalam satu tempat yang sama dan berjarak kurang dari 1 kilometer sehingga menciptakan suatu jaringan tersendiri. Gambaran umum dari LAN dapat dilihat dari gambar 2.1.



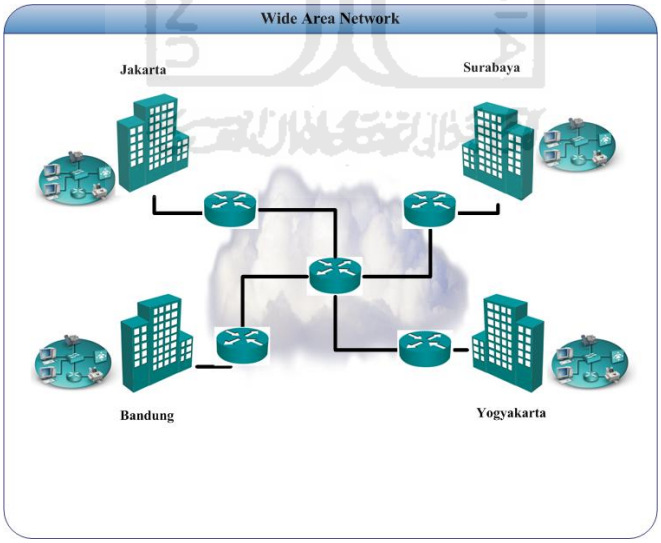
Gambar 2. 1 Koneksi *Local Area Network* (LAN)

Metropolitan Area Network (MAN) adalah gabungan dari beberapa jaringan LAN yang terpisah tempat yang berbeda dan secara letak masih dalam di kota yang sama. Gambaran umum dari MAN dapat dilihat dari gambar 2.2.



Gambar 2. 2 Koneki *Metropolitan Area Network* (MAN)

Wide Area Network (WAN) adalah kumpulan dari LAN dan/atau Workgroup yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan Internet, dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang [SHP00]. Gambaran umum tentang WAN dapat dilihat di gambar 2.3.



Gambar 2. 3 Koneksi *Wide Area Network* (WAN)

WAN banyak digunakan untuk menghubungkan beberapa tempat yang berbeda jarak agar bisa saling berkomunikasi secara langsung. WAN dapat diklasifikasikan sebagai berikut:

1. Private WAN Merupakan implementasi WAN yang menggunakan jaringan khusus atau tidak bisa digunakan oleh orang lain. Contoh dari private WAN adalah dedicated WAN(*leased line*) dan Shared WAN.
2. Publik WAN Merupakan implementasi WAN yang dapat menggukan jaringan publik atau Internet.

Penggunaan private WAN membutuhkan investasi yang sangat besar., disebabkan penggunaan jaringan secara khusus tanpa digunakan oleh pihak lain. Salah satu solusi untuk menghemat biaya dalam implementasi WAN adalah penggunaan publik WAN. Penggunaan publik WAN dapat menghemat biaya implementasi disebakan penggunaan jaringan publik atau Internet sebagai koneksi utama.

Kelemahan penggunaan publik WAN adalah masalah keamanan yang sangat jauh dari level aman, banyaknya orang yang tidak bertanggung jawab dalam penggunaan Internet membuat resah banyak pihak [OWP11]. Maka dipilihlah koneksi *Virtual Private Network* (VPN) yang mengunakan media Internet sebagai koneksi kekantor cabang.

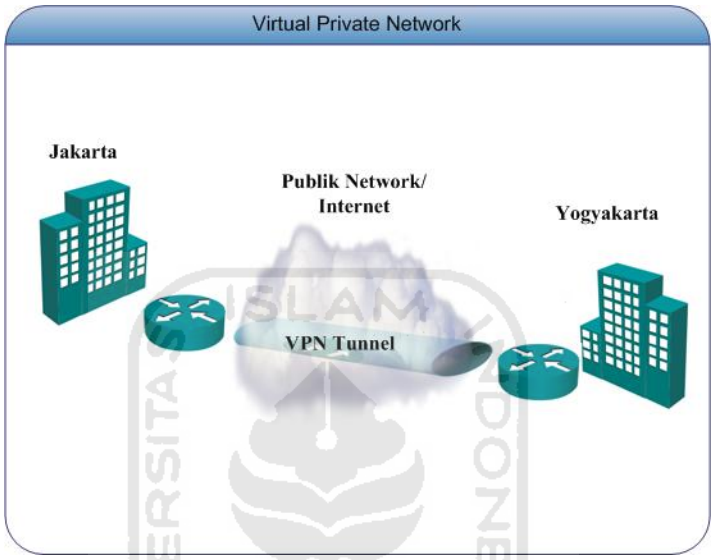
2.2 Virtual Private Network (VPN)

2.2.1 Definisi VPN

Virtual Area Network (VPN) merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik. Infrastruktur publik yang paling banyak digunakan adalah Internet. Untuk memperoleh komunikasi yang aman (*private*) melalui Internet, diperlukan protokol khusus untuk mengatur pengamanan datanya [MHS04].

Metode penggunaan VPN untuk koneksi WAN yang menggunakan media Internet merupakan salah satu Solusi alternatif jaringan skala luas saat ini bisa menggunakan VPN yang lebih ekonomis dan tepat. Teknologi VPN dapat

memberikan keamanan di dalam melakukan komunikasi data melalui jaringan Internet serta merupakan solusi yang efisien dan ekonomis dibandingkan dengan teknologi jaringan skala luas lainnya [OWP11]. Gambaran umum implementasi WAN menggunakan media VPN dapat dilihat pada gambar 2.4.



Gambar 2. 4 Skema VPN(*Virtual Private Network*)

Kelebihan dan Kekurangan VPN

VPN memiliki beberapa kekurangan dan kelebihan yang harus di antisipasi pada saat ingin melakukan implementasi yaitu:

1. Kelebihan
   a. Biaya relatif murah.

      VPN merupakan teknologi yang dibangun dengan memanfaatkan jaringan Internet tanpa perlu membangunkan jaringan pribadi. Dengan demikian, hanya sambungan ke Internet diperlukan untuk menggunakan VPN, sehingga biaya yang diperlukan secara relatifnya lebih murah [MHS04].

   b. Fleksibilitas.

      VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke Internet. Sehingga pegawai yang *mobile* dapat mengakses

jaringan khusus perusahaan dimanapun dia berada. Selama dia bisa mendapatkan akses ke Internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan [MHS04].

c. Mudah diatur.

Keseluruhan VPN dapat diatur dalam server VPN sendiri, dan untuk dapat digunakan oleh klien, maka perlu diinstal aplikasi VPN pada klien [MHS04].

d. Mengurangi kerumitan pengaturan dan teknologi *tunneling*.

Tunneling atau terowongan merupakan kunci utama pada VPN. Sambungan pribadi dalam VPN dapat terjadi di mana saja selama terdapat tunnel yang menghubungkan pengirim dan penerima data. Dengan adanya tunnel ini, maka tidak diperlukan pengaturan-pengaturan lain yang ada diluar tunnel tersebut, asalkan sumber dari tunnel tersebut dapat menjangkau tujuannya [MHS04].

2. Kekurangan

a. VPN membutuhkan perhatian yang serius pada keamanan jaringan publik (Internet). Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN [MHS04].

b. Ketersediaan dan performansi jaringan khusus perusahaan melalui media Internet sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan. Kecepatan dan keandalan transmisi data melalui Internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur oleh pihak pengguna jaringan VPN, karena *traffic* yang terjadi di Internet melibatkan semua pihak pengguna Internet di seluruh dunia [MHS04].

c. Perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda ada kemungkinan tidak dapat digunakan secara bersama-sama karena standar yang ada untuk teknologi VPN belum memadai. Oleh karena itu fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan dan keuangan perusahaan sangat kurang. [MHS04]

2.2.2 Tunneling

Tunneling adalah suatu mekanisme enkapsulasi dengan membentuk jaringan baru secara *private* diatas jaringan publik dengan cara pembungkusan payload pada frame *Point to Point Protocol* (PPP) untuk dilewatkan pada jaringan [OWP11]. Pada jaringan VPN ada 2 jenis *tunneling* yang digunakan, *layer* 2 *Tunneling* dan *layer* 3 *Tunneling*.

Pada *layer* 2 *tunneling* layanan yang diberikan berupa koneksi antar komputer yang tempatnya berbeda jarak. *Layer* 2 *tunneling* tidak memungkinkan komunikasi antar komputer yang berbeda jaringan. Contoh dari *layer* 2 *tunneling* adalah L2TP dan PPTP.

Layer 3 *tunneling* merupakan solusi penggunan VPN untuk jaringan yang berskala besar. *Layer* 3 *tunneling* memungkinkan komunikasi antar komputer yang berbeda jaringan. *Layer* 3 *tunneling* merupakan solusi terbaik dalam penggunaan VPN pada jaringan yang berskala besar. Contoh dari *layer* 3 *Tunneling* adalah GRE dan MPLS.

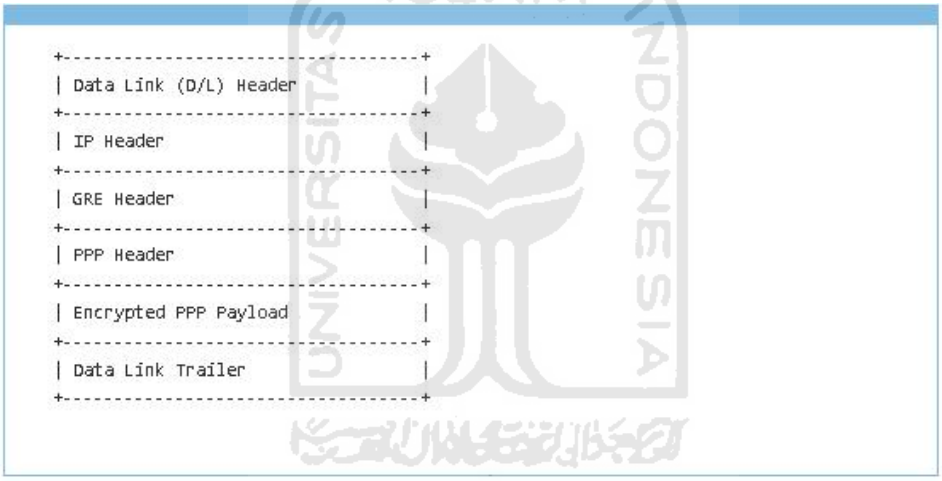
2.2.3 Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE**)** merupakan mekanisme protokol *tunneling* yang dikembangkan oleh Cisco System yang dapat dilewati berbagi paket data dengan cara membuat tunnel atau jalan khusus berbentuk point-to-point [FAR11].

Implementasi GRE hanya bisa dilakukan oleh *router gateway*, hal ini dikarenakan penggunaan GRE dapat melibatkan proses routing dalam *tunnel* GRE. Sehingga dengan adanya proses routing tersebut GRE memungkinkan komunikasi berbeda jaringan yang cukup besar. Pada gambar 2.5 akan mengambarkan topologi GRE.

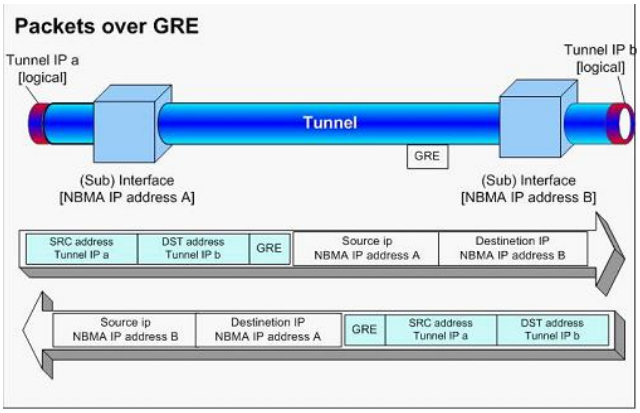
Gambar 2. 5 Topologi *Generic Routing Encapsulation*(GRE)

Pada topologi jaringan yang meggunakan *tunnel* GRE, proses pengiriman paket data akan dienkapsulasi secara otomatis oleh gateway yang terinstall GRE. Format enkapsulasi dapat dilihat pada gambar 2.6 yang diambil dari [MRS41]

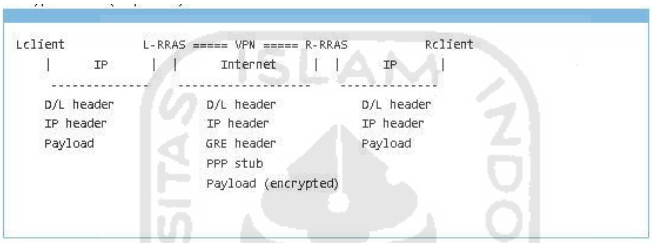


Gambar 2. 6 Format *Encapsulation* GRE

Ketika paket data dikirimkan dari router a ke router b menggunakan *tunnel* GRE, GRE melakukan proses enkapsulasi untuk menciptakan *tunnel* sebagai jalur data khusus untuk meneruskan paket melalui jaringan komputer, baik itu jaringan komputer pribadi ataupun publik. Pada gambar 2.7 dan gambar 2.8 yang diambil dari [MRS41] akan dijelaskan poses enkapsulasi pada pengiriman data menggunakan *tunnel* GRE.



Gambar 2. 7 Proses enkapsulasi data pada GRE



Gambar 2. 8 Proses enkapsulasi data GRE

GRE *tunnel* merupakan metode *tunneling* yang tidak memiliki enkripsi sebagai protokol keamanan. Oleh karena dibutuhkan sebuah protokol kemanan salah satunya *IP Security* (IPSec)

2.2.4 IP Security (IPSec)

IP Security (IPSEC) adalah sebuah *framework* standar terbuka yang dikembangkan oleh Internet Engineering Task Force (IETF). IPSec menyediakan keamanan untuk transmisi informasi yang bersifat sensitif melalui jaringan yang tanpa proteksi seperti Internet. IPSec dijalankan pada layer network pada jaringan, berfungsi untuk melindungi dan melakukan otentikasi paket IP antara perangkat IPSec

IPSec menyediakan servis jaringan keamanan berikut ini. Servis-servis berikut ini bersifat opsional. Pada umumnya, kebijakan keamanan lokal yang akan menentukan penggunaan salah satu atau lebih servis berikut:

1. Data Confidentiality, yaitu pengirim IPSec dapat mengenkripsi paket sebelum mentransmisikannya melalui sebuah jaringan, untuk meyakinkan informasi yang dikirimkan tidak dapat dibaca oleh orang yang tidak berhak. Algoritma enkripsi yang digunakan seperti NULL, DES, 3DES, AES dan Blowfish.
2. Data Integrity, yaitu penerima IPSec dapat melakukan otentikasi paket yang dikirim oleh pengirim IPSec untuk memastikan bahwa data tidak diubah selama proses transmisi. IPSec menerapkan *Hash Message Authentication Codes (HMAC)*, dengan *hash algorithms* seperti MD5 dan SHA.
3. Data Origin Authentication, yaitu penerima *IPSec* dapat melakukan otentikasi terhadap sumber dari paket *IPSec* yang dikirim. Servis ini tergantung pada layanan integritas data. Dengan definisi *secret Key*, dalam karakter ascii dan hexadesimal.
4. Anti-Replay, yaitu penerima *IPSec* dapat mendeteksi dan menolak paket yang dikirim berulang.

IPSec menggunakan 2 protokol, dengan layanan:

1. Authentication Header (AH): memungkinkan verifikasi identitas pengirim. AH juga memungkinkan pemeriksaan integritas dari pesan/informasi, atau AH menyediakan servis data integrity dan origin authentication.
2. Encapsulating Security Payload (ESP): memungkinkan enkripsi informasi sehingga tetap rahasia, istilah lainnya menyediakan servis data confidentiality.

AH dan ESP mendukung dua mode yang dapat digunakan, yaitu: mode *transport* dan mode *tunnel*. Mode *transport* menyediakan pengamanan terutama untuk protokol layer yang lebih tinggi. Pada mode *transport*, sebuah header IPSec (AH atau ESP) disisipkan setelah *header* IP dan sebelum header protokol layer yang lebih tinggi dan data user.

Pada mode *tunnel*, keseluruhan datagram IP dienkapsulasi dalam sebuah paket IPSec yang baru (sebuah *header* IP baru yang diikuti dengan sebuah *header* AH atau ESP). Menciptakan *tunnel* dalam jaringan yang tidak terhubung secara langsung. Sebuah *tunnel* diciptakan melalui jaringan publik seperti Internet. Jadi seolah-olah ada hubungan *point-to-point* dengan data yang dienkapsulasi. Dalam mode *tunneling*, IPSec bisa dipergunakan untuk pengenkapsulasian paket. IPSec juga bisa dipergunakan untuk enkripsi dalam protokol *tunneling* lainnya.

Pengamananan hubungan dalam IPSec didefinisikan dalam istilah *security associations* (SA). SA ini disimpan juga dalam *security association database* (SAD). Tiap SA mendefinisikan satu hubungan data secara unidirectional. Parameter yang digunakan dalam SA adalah sebagai berikut:.

1. Alamat IP sumber dan tujuan berupa IPsec *header* hasil enkapsulasi, yaitu alamat IP dari *IPSec Peers.*
2. Protokol IPSec (AH or ESP).
3. Kekuatan Algoritma dan *Secret Key* yang digunakan.
4. *Security Parameter Index* (SPI), sebesar 32 bit.

Secara bersama protokol IPSec AH dan ESP menyediakan privasi, integritas, dan autentifikasi dari paket IP, namun hal tersebut belum lengkap. IETF juga telah menyediakan protokol yang melayani negosiasi antar protokol IPSec, algoritma, dan kunci dalam komunikasi tersebut, verifikasi identitas, dan mengatur pertukaran kunci.

Internet security association and key management protocol (ISAKMP) secara otomatis mengatasi pertukaran kunci rahasia antara pengirim dan penerima. Protokol tersebut memadukan ISAKMP dengan metode *Oakley*. ISAKMP biasa disebut juga *Internet key exchange* (IKE).

ISAKMP didasarkan atas model pembangkitan kunci Diffie-Hellman, dimana dua entitas saling berbagi informasi sebelum yakin identitas entitas yang lainnya. Dengan Diffie-Hellman, dua entitas membangkitkan nilai publik mereka, yang kemudian mereka kirim ke entitas yang lain. Tiap entitas mengambil kunci

publik yang telah diterima dan mengkombinasikannya dengan kunci yang ada. Hasilnya seharusnya sama untuk kedua entitas.

ISAKMP mendukung tiga metode pertukaran kunci yaitu: *main mode*, *aggressive mode*, dan *quick mode*. *Main mode* membangun yang dikenal sebagai fasa pertama dari ISAKMP SA. SA atau *security association*, adalah metode untuk menyimpan semua detail mengenai kunci dan algoritma dalam tiap sesi IPSec. SA mencakup informasi yang sangat luas, termasuk algoritma autentifikasi AH dan kunci, algoritma enkripsi ESP dan kunci, berapa sering kunci harus diganti, bagaimana komunikasi di autentifikasi, dan informasi tentang umur SA.

Main mode membangun sebuah mekanisme yang digunakan untuk komunikasi diwaktu mendatang. Pada main mode persetujuan dalam autentifikasi, algoritma, dan kunci dilakukan. Main mode membutuhkan tiga tahap pertukaran antara pengirim dan penerima. Langkah pertama, dua entitas setuju dalam menggunakan algoritma dan hash untuk komunikasi. Langkah kedua, bertukar kunci publik menggunakan model pertukaran Diffie-Hellman dan kemudian membuktikan identitas mereka kepada yang lain. Langkah terakhir, penerima dan pengirim saling memverifikasi identitas.

Pada *aggressive mode* sama dengan *main mode* hanya saja jumlah langkah yang dilakukan dua langkah saja, dan yang terakhir pada *quick mode* dimana dapat digunakan setelah SA dan ISAKMP telah dibuat menggunakan *main mode* atau *aggressive mode* untuk membuat material baru untuk membangkitkan kunci. Ini dikenal sebagai fasa pertukaran kedua. Dalam *quick mode*, semua paket telah dienkripsi, jadi langkah ini lebih mudah dari *main mode* dan *aggressive mode.*

Cara kerja IPSec dapat dibagi dalam lima tahap, yaitu:

1. Memutuskan menggunakan IPSec antara dua titik akhir di Internet.
2. Mengkonfigurasi dua buah *gateway* antara titik akhir untuk mendukung IPSec.
3. Inisialisasi tunnel IPSec antara dua gateway.
4. Negosiasi dari parameter IPSec/IKE antara dua gateway.
5. Mulai melewatkan data.

Dari tahapan tersebut ada bagian yang menarik jika diperhatikan proses handshakingnya, sebelumnya telah disinggung bahwa ISAKMP-IKE menerapkan dua mode yaitu *main mode* dan *aggressive mode*. Kedua mode tersebut mempunyai cara yang berbeda dalam terjadinya koneksi IPSec.

2.3 VOIP (Voice Over Internet Protocol)

Kebutuhan akan komunikasi sudah merupakan kebutuhan utama bagi semua orang. *Voice Over Internet Protocol* (VOIP) merupakan sebuah solusi komunikasi yang menggunakan media Internet. Keuntungan penggunaan VOIP adalah biaya lebih rendah dalam penggunaan. Penggunaan VOIP pada perusahaan sangat membantu dalam penghematan biaya. Penggunaan VOIP dalam komunikasi kantor pusat ke kantor cabang dapat dilalui pada topologi GRE over IPSec.

Penggunaan VOIP pada GRE over IPSec menitikberatkan pada performa dan kualitas suara yang diberikan. Penggunaan VOIP dalam GRE over IPSec harus memenuhi standar kualitas. Parameter standar kualitas VOIP diantaranya:

1. Delay

   Dalam perancangan jaringan VoIP, delay merupakan suatu permasalahan yang harus diperhitungkan karena kualitas bagus tidaknya suara tergantung dari waktu delay. Besarnya delay maksimum yang direkomendasikan oleh *International Telecommunication Union* (ITU) untuk aplikasi suara adalah 150 ms, sedangkan delay maksimum dengan kualitas suara yang masih dapat diterima pengguna adalah 250 ms [MHS11].

2. Jitter

   Jitter merupakan variasi dari delay. Jitter dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan. Pengaruh jitter pada kinerja jaringan harus dilihat bersama delay. Ketika jitter besar namun delay-nya kecil maka kinerja jaringan tidak bisa dikatakan jelek karena besarnya jitter dapat dikompensasi dengan nilai

delay yang kecil. Jitter akan menurunkan kinerja jaringan ketika nilainya besar dan juga nilai delay-nya juga besar [MHS11].

3. Paket loss

Merupakan suatu keadaan dimana suatu paket tidak sampai ketujuan atau gagal ketujuan [MHS11].

2.4 File Transfer Protocol (FTP)

File Trasnfer Protocol (FTP) adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) komputer antar mesin-mesin dalam sebuah *Internetwork*. FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (*download*) dan penggugahan (*upload*) berkas-berkas komputer antara klien FTP dan server FTP [POS11].

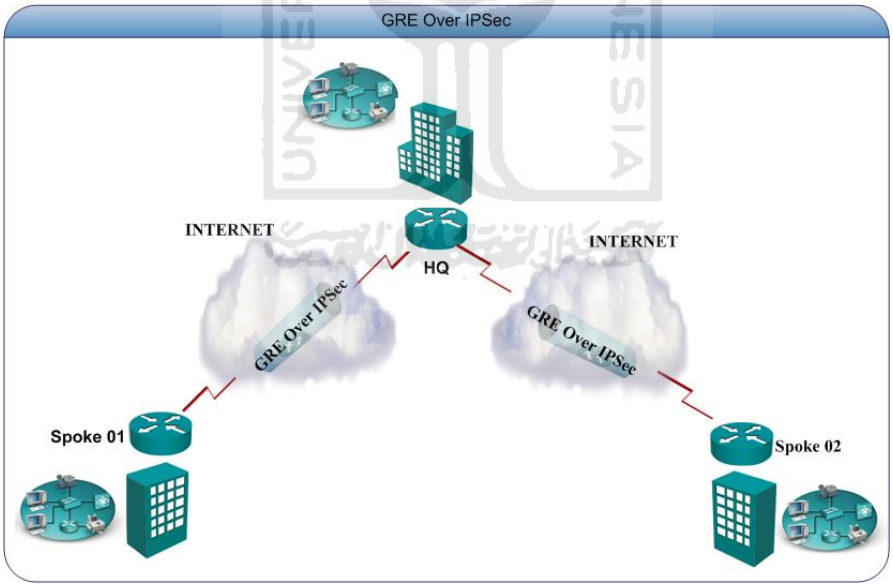
2.5 Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) dibuat untuk mengirimkan pesan pengujian dan kontrol antara alamat *Internet Protocol* (IP) yang berbeda. Dalam hal ini ICMP digunakan oleh sistem operasi jaringan komputer untuk mengirim pesan sebagai salah satu alternative yang dapat menunjukan bahwa komputer tersebut dapat dihubungi atau tidak.

BAB III
METODOLOGI

3.1 Analisa Sistem

Implemantasi GRE mengacu pada komunikasi antara beberapa korporat dalam suatu jaringan yang saling terintegrasi. Komunikasi data tersebut menitikberatkan pada faktor keamanan yang terbentuk melalui *tunnel* GRE Over IPSec sehingga pihak pengguna layanan tidak perlu khawatir akan sisi keamanan paket data yang dilewatkan. Dengan mengabaikan proses routing yang disediakan oleh provider penyedia jasa Internet (ISP), pihak korporat hanya mengetahui proses integrasi antar node perusahaan yang terbagi dalam jangkauan wilayah yang sangat luas. Gambaran umum implementasi GRE dapat dilihat pada gambar 3.1 berikut:.



Gambar 3. 1 Gambaran umum GRE Over IPSec

Pada gambar 3.1 diatas, Head Quarter (HQ) atau disebut juga kantor pusat, terintegrasi oleh dua buah kantor cabang (*Spoke*) melalui Internet dengan media keamanan VPN. Diantara HQ dan dua buah *spoke* tersebut terhubung secara

khusus melalui *tunnel* GRE over IPSec. Skema komunikasi yang terbentuk antara kedua *spoke* dan HQ tersebut membentuk suatu jaringan private yang menggambarkan hubungan antara satu buah korporat pusat dengan dua buah kantor cabang.

3.1.1 Implementasi Sistem

1. Perangkat lunak Sistem

Perangkat lunak yang dibutuhkan adalah sebagai berikut:

1. GNS3.

   GNS3 adalah simulator cisco berbasis grafik yang bisa jalan di windows dan linux. mngkin kita pernah pakai dynagen dan dynamips untuk membuat cisco lab.

2. VMWARE.

   VMWARE adalah plikasi untuk membuat mesin dan OS virtual.

3. Wireshark.

   Wireshark adalah program yang berfungsi untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi dengan jaringan.

4. WinPcap.

   WinPcap adalah perangkat jaringan standar industri yang berjalan di network layer pada lingkungan kerja windows.

5. X-lite.

   X-lite adalah aplikasi softphone yang bisa digunakan dengan berbagai macam operator telepon.

6. VQManager.

   VQManager adalah Aplikasi monitoring serta penganalisa sistem VoIP serta kualitas suara yang dihasilkan.

7. Asterisk.

   Asterisk adalah likasi open source PBX (*Private Branche eXchange*) yang memungkinkan komunikasi antar pengguna telepon regular maupun telepon berbasis sip (sip phones).

8. FileZilla.

   FileZilla adalah aplikasi client dan server FTP yang memiliki sejumlah fitur dan antarmuka nan memudahkan transfer file lebih dari satu secara bersamaan sehingga proses transfer banyak file dapat berjalan dengan cepat

2. Perangkat Keras Sistem

Komponen perangkat keras yang akan disimulasikan adalah sebagai berikut:

1. Router Cisco seri 7200.

   Router Cisco seri 7200 digunakan pada router gateway yang menghubungkan antara kantor pusat (HQ) dan cabang (SPOKE)

2. Windows XP.

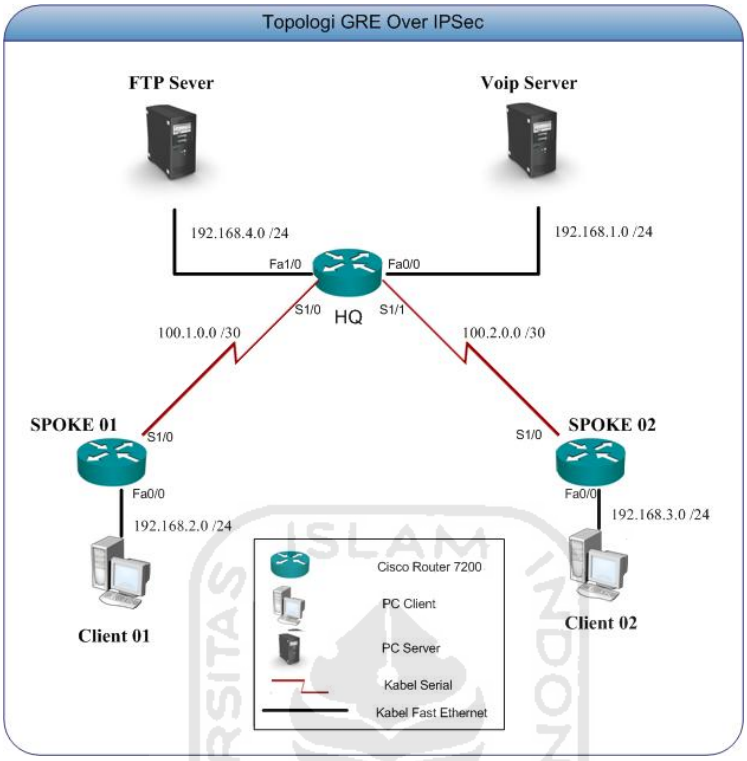
   Sistem operasi Windows XP digunakan sebagai server FTP dan klien

3. Server VOIP.

   Server VOIP menggunkan server Briker IPPBX 1.04. Server Briker berbasis linux Ubuntu dan menggunakan asterisk pada aplikasi VOIP.

3.1.2 Topologi Jaringan

Implementasi yang akan dilakukan yaitu melakukan simulasi GRE Over IPSec menggunakan router seri 7200, topologi pada simulasi dapat dilihat pada gambar 3.2.



Gambar 3. 2 Topologi GRE Over IPSec

Dari gambar 3.2 diatas, parameter alokasi alamat IP yang akan dibangun adalah sebagai berikut:

Tabel 3. 1 Alokasi alamat IP

Nama Perangkat	Interface	Alamat IP
HQ	Serial 1/0	100.1.0.1
	Serial 1/1	100.2.0.1
	Fast Ethernet 0/0	192.168.1.1
	Fast Ethernet 0/1	192.168.4.1
	Tunnel 0	10.1.0.1
	Tunnel 1	10.2.0.1
SPOKE_01	Serial 1/0	100.1.0.2
	Fast Ethernet 0/0	192.168.2.1
	Tunnel 1	10.1.0.2
SPOKE_02	Serial 1/0	100.2.0.2
	Fast Ethernet 0/0	192.168.3.1
	Tunnel 0	10.2.0.2
VOIP Server	Fast Ethernet	192.168.1.2

Nama Perangkat	Interface	Alamat IP
FTP Server	Fast Ethernet	192.168.4.2
PC Klien 01	Fast Ethernet	192.168.2.2
PC Klien 02	Fast Ethernet	192.168.3.2

3.1.3 Konfigurasi

Topologi GRE Over IPSec membutuhkan konfigurasi di beberapa tempat untuk dapat menghubungkan setiap perangkat yang saling terintegrasi dengan metode GRE Over IPSec.

1. Konfigurasi HQ

Mengacu pada gambar 3.1, pada router HQ akan dilakukan konfigurasi alamat ip pada *Interface FastEhternet 0/0, Interface FastEhternet 0/1, Interface Serial 1/I,* dan *Interface Serial 1/1*. Konfigurasinya yang dibuthkan adalah sebagai berikut:.

```
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 192.168.4.1 255.255.255.0
!
interface Serial1/0
 bandwidth 128
 ip address 100.1.0.1 255.255.255.252
 clock rate 9600
!
interface Serial1/1
 bandwidth 128
 ip address 100.2.0.1 255.255.255.252
!
```

Konfigurasi selanjutnya adalah menentukan parameter *Internet Security Accociation and Key Management Protocol* (ISAKMP). Hal ini berguna untuk proses autentikasi yang akan digunakan. *Internet Key Exchange* (IKE) yang digunakan adalah “Cisco” dan langsung memberikan IP tujuan.

```
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 7200
crypto isakmp key Cisco address 100.1.0.2 no-xauth
crypto isakmp key Cisco address 100.2.0.2 no-xauth
!
```

Setelah menentukan parameter ISKMP, selanjutnya adalah melakukan konfigurasi pada sisi *transform Set.* Hal ini berfungsi untuk melakukan definisi pada sisi IPSec untuk memilih protokol enkripsi yang digunakan. Protokol enkripsi yang digunakan adalah “ESP, AES, SHA, dan HMAC”.

```
!
crypto ipsec transform-set HQ esp-aes esp-sha-hmac
!
```

Selanjutnya menentukan konfigurasi pada ISAKMP dan *transform Set* dengan melakukan konfigurasi pada sisi Profil. Profil pada IPSec yang berfungi untuk melakukan kombinasi pada ISAKMP, *transfom Set* dan IKE agar bekerja secara bersamaan. Profil yang digunakan adalah “IPSEC_PROFILE”.

```
!
crypto ipsec profile IPSEC_PROFILE
 set transform-set HQ
!
```

Konfigurasi selanjutnya adalah konfigurasi GRE dengan menggunakan *Interface Tunnel.* Pada konfigurasi ini terdapat fitur untuk memanggil IPSec yang sudah dikonfigurasi sebelumnya. "*Tunnel Mode ipsec ipv4"* berfungsi untuk memastikan bahwa tunnel yang ada akan diencapsulasi oleh IPSec, sedangkang "*tunnel protection ipsec profile IPSEC_PROFILE"* bertujuan untuk memanggil IPSec dengan nama profil "IPSEC_PROFILE".

```
!
interface Tunnel0
 ip address 10.1.0.1 255.255.255.252
 tunnel source Serial1/0
 tunnel destination 100.1.0.2
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile IPSEC_PROFILE
!
interface Tunnel1
 ip address 10.2.0.1 255.255.255.252
 tunnel source Serial1/1
 tunnel destination 100.2.0.2
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile IPSEC_PROFILE
!
```

Konfigurasi selanjutnya adalah melakukan konfigurasi pada sisi routing. Ini bertujuan agar semua jaringan yang ada dapat terhubung dengan sempurna. Routing Protokol yang di gunakan adalah "EIGRP".

```
!
router eigrp 1
 network 10.1.0.1 0.0.0.0
 network 10.2.0.1 0.0.0.0
 network 192.168.1.0
 network 192.168.4.0
 auto-summary
!
```

2. Konfigurasi SPOKE_01

Konfigurasi pada router SPOKE_01 dimulai dari konfigurasi *interface fastEthernet dan Interface Serial.* Alokasi alamat ip bisa dilihat pada table 3.1.

```
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
!
interface Serial1/0
 bandwidth 128
 ip address 100.1.0.2 255.255.255.252
!
```

Konfigurasi ISAKMP pada SPOKE_01 menggunakan ”Cisco” sebagai IKE sama seperti *router* HQ.

```
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 7200
crypto isakmp key Cisco address 100.1.0.1 no-xauth
!
```

Pada Konfigurasi *transform Set* pada menggunakan metode enkripsi yang sama dengan HQ. Perbedaan konfigurasi pada sisi *transform set* antara router HQ denga router SPOKE_01 ada dipenamaan. Penamaan yang digunakan “SPOKE_01”.

```
!
crypto ipsec transform-set SPOKE_01 esp-aes esp-sha-hmac
!
```

Untuk konfgurasi pada sisi Profile sama seperti HQ yang membedakan hanya nama pada sisi *transform set* disebab kan mengikuti konfigurasi pada sisi *transform set.*

```
!
crypto ipsec profile IPSEC_PROFILE
 set transform-set SPOKE_01
!
```

Pada Konfigurasi tunnel sama seperti konfigurasi pada *router* HQ.Yang membedakan pada alokasi IP *address.*

```
!
interface Tunnel0
 ip address 10.1.0.2 255.255.255.252
 tunnel source Serial1/0
 tunnel destination 100.1.0.1
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile IPSEC_PROFILE
!
```

Konfigurasi pada sisi routing menggunakan routing protokol “EIGRP”.

```
!
router eigrp 1
 network 10.1.0.2 0.0.0.0
 network 100.0.0.0
 network 192.168.2.0
 no auto-summary
!
```

3. Konfigurasi SPOKE_02

Pada *router* SPOKE_02 konfigurasi alamat ip yang digunakan seperti pada table 3.2. *Interface* yang akan dikonfigurasi adalah *interface FastEtherner* dan *Interface Serial*.

```
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
!
interface Serial1/0
 bandwidth 128
 ip address 100.2.0.2 255.255.255.252
!
```

Konfigurasi pada sisi ISAKMP yang digunakan pada router SPOKE_02 adalah sebagai berikut:

```
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 7200
crypto isakmp key Cisco address 100.2.0.1 no-xauth
!
```

Untuk konfigurasi pada sisi transform Set pada router SPOKE_02 adalah sebagai berikut:

```
!
crypto ipsec transform-set SPOKE_02 esp-aes esp-sha-hmac
!
```

Konfigurasi selanjutnya pada sisi profil pada router SPOKE_02 adalah sebagai berikut:

```
!
crypto ipsec profile IPSEC_PROFILE
 set transform-set SPOKE_02
!
```

Lanjut konfigurasi pada sisi tunnel GRE pada sisi router SPOKE_02 adalah sebagi berikut:

```
!
interface Tunnel0
 ip address 10.2.0.2 255.255.255.252
 tunnel source Serial1/0
 tunnel destination 100.2.0.1
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile IPSEC_PROFILE
!
```

Konfigurasi selanjutnya pada router SPOKE_02 melakukan konfigurasi pada sisi routing.

```
!
router eigrp 1
 network 10.2.0.2 0.0.0.0
 network 100.0.0.0
 network 192.168.2.0
 no auto-summary
!
```

4. Konfigurasi VOIP Server

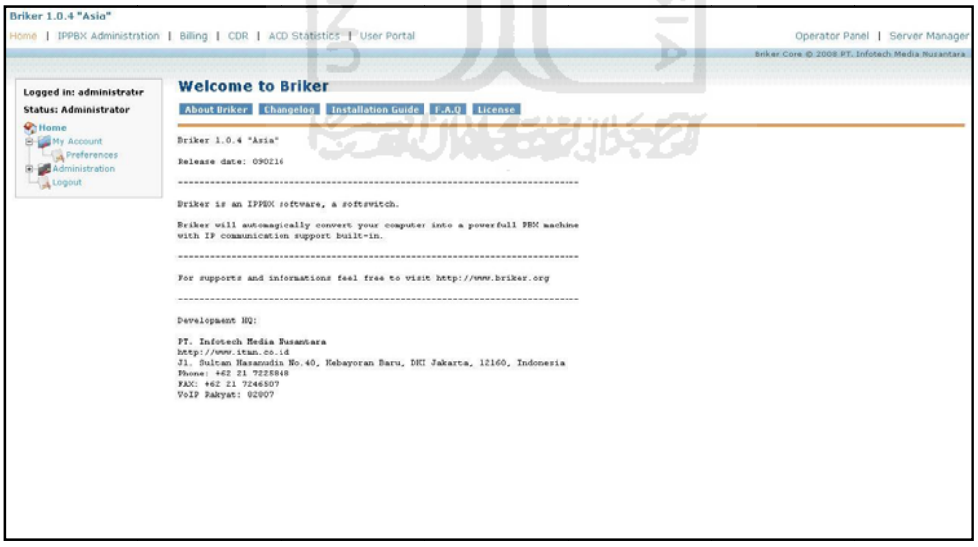
Voip server yang digunakan pada implementasi VPN menggunkan GRE Over IPSec, menggunakan server Briker IPPBX 1.04. Server Briker berbasis linux Ubuntu dan menggunakan asterisk pada aplikasi VOIP. Konfigurasi alamat IP adalah sebagai berikut:

```
auto eth0
iface eth0 inet static
    address 192.168.2.2
    netmask 255.255.255.0
    network 192.168.2.0
    broadcast 192.168.2.255
    gateway 192.168.2.1
```

Konfigurasi lebih lanjut dapat dilakukan melalui GUI yang sudah terinstall secara otomatis. GUI dapat diakses melalui web browser dengan mengetikan alamat IP server. Pada gambar 3.3 menampilkan halaman login pada server voip.

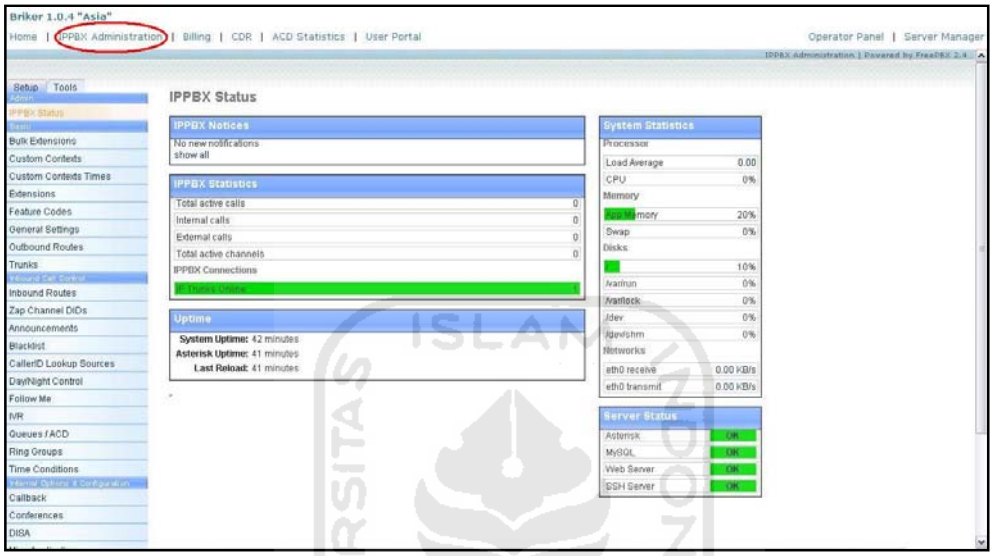
Gambar 3. 3 Halaman Login Voip

Untuk masuk kedalam sistem dibutuhkan login. Username yang digunakan adalah “administrator” dan password yang digunakan adalah “Briker”. Ketika berhasil untuk login kedalam sistem akan masuk kedalam menu home. Pada gambar 3.4 akan menampilkan menu home.



Gambar 3. 4 Tampilan pada menu *Home*

Untuk menuju halaman IPPBX Administration yang dipergunakan untuk melihat IPPBX Status pilih menu IPPBX Administration pada *toolbar*. Dapat dilihat pada Gambar 3.5.

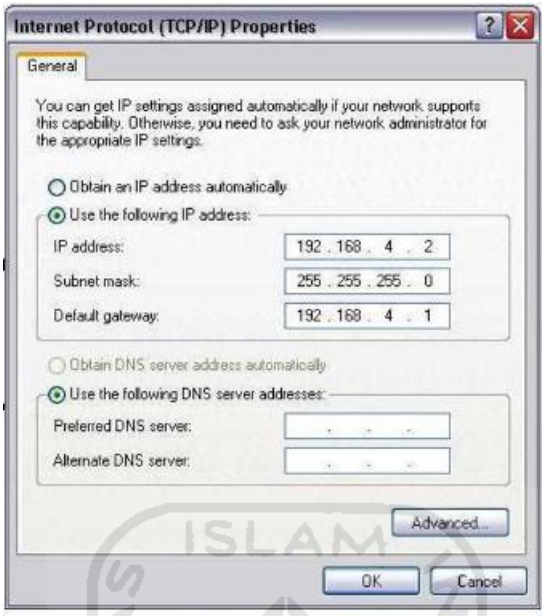


Gambar 3. 5 Tampilan pada menu *IPPBX Administration*

Konfigurasi yang selanjutnya adalah membuat user pada voip server yang dipergunakan supaya setiap klien dapat terdaftar didalam sistem. Menu yang digunakan pada sesi ini adalah menu Extensions. Pada gambar 3.6 menampilkan menu Extensions.

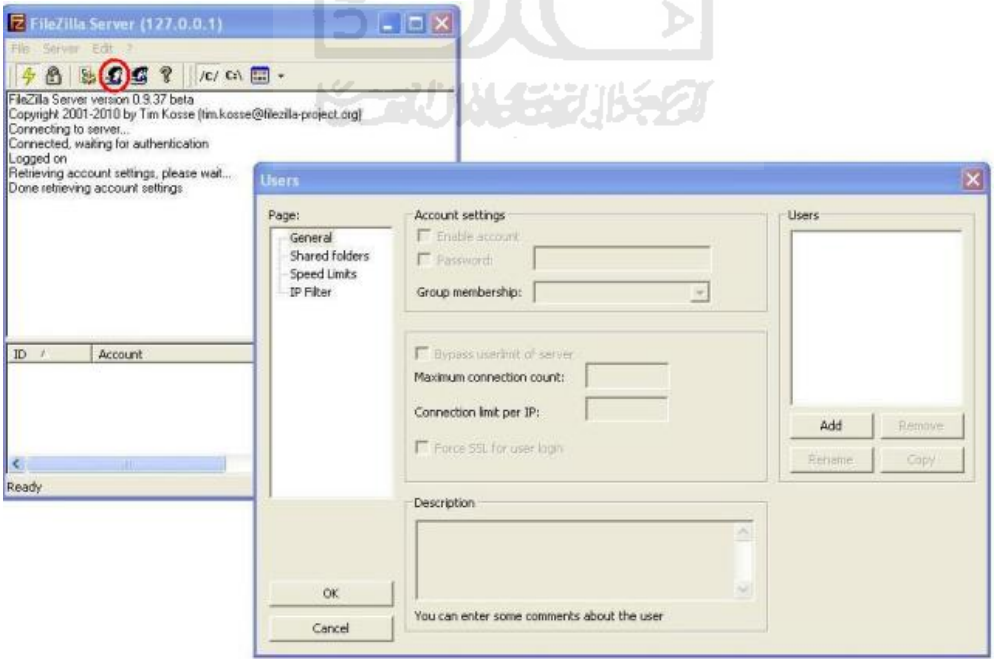
5. Konfigurasi FTP Server

Server FTP yang digunakan menggukan aplikasi FileZilla-Sever yang menggunakan windows xp sebagai sistem operasinya. Langkah pertama melakukan konfigurasi pada alamat ip seperti pada gambar 3.10.



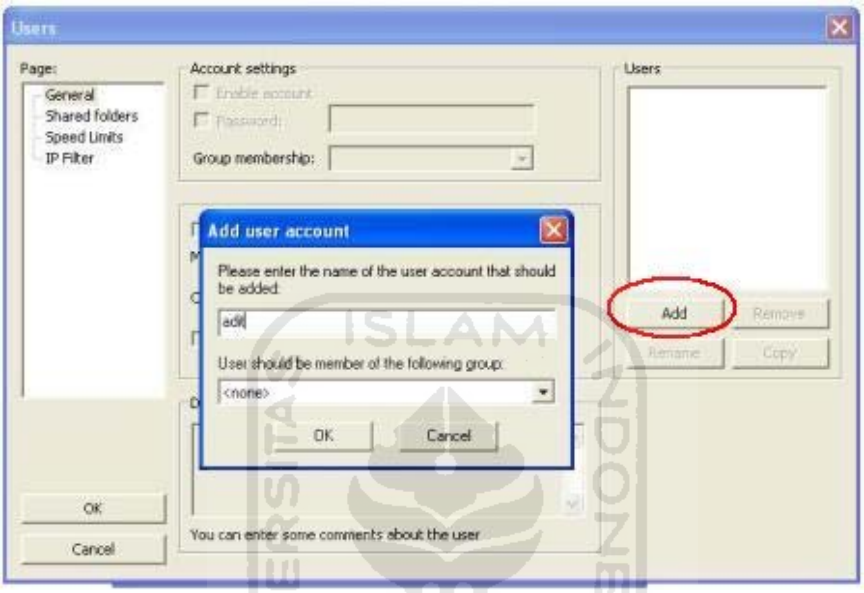
Gambar 3. 6 Konfigurasi IP address pada FTP server

Selanjutnya melakukan konfigurasi untuk membuat user yang berhak untuk menggunakan fasilitas FTP. Akan di jelaskan pada gambar 3.11.

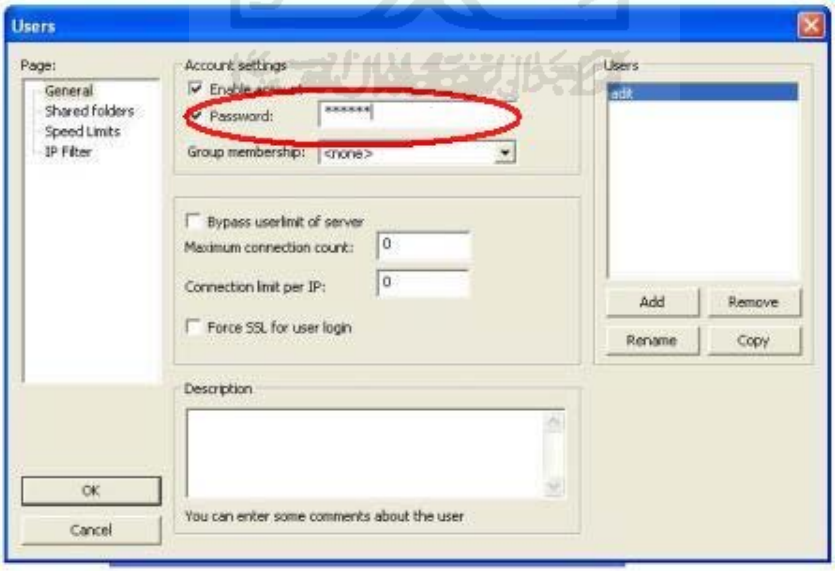


Gambar 3. 7 Menu untuk membuat user

Pada menu pembuatan user dengan memasukan nama user dan password. Nama user yang digunakan adalah “adit” dan password yang akan digunakan adalah “123456”. Seperti pada gambar 3.12 dan gambar 3.13.

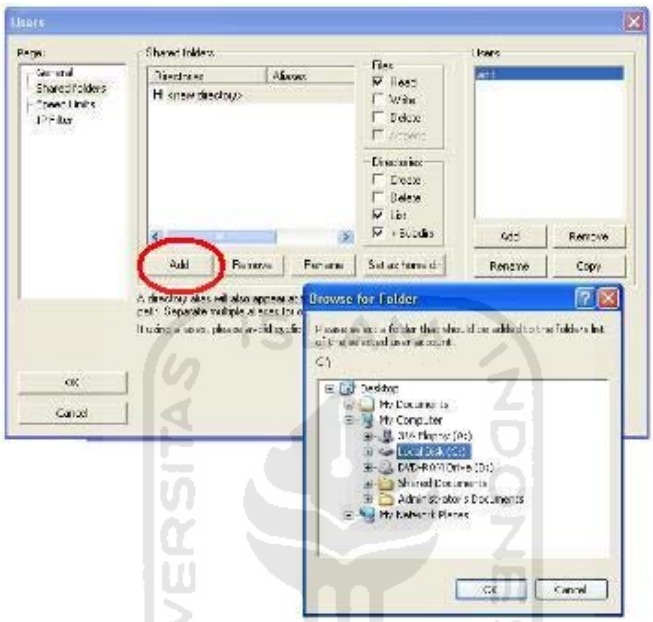


Gambar 3. 8 Pembuatan User



Gambar 3. 9 Pembuatan password

Sesudah user terbentuk, langkah selanjutnya mengkonfigurasi atau lokasi penyimpanan *file* FTP. Gambar 3.14 menjelaskan konfigurasi peletakan lokasi penyimpanan.

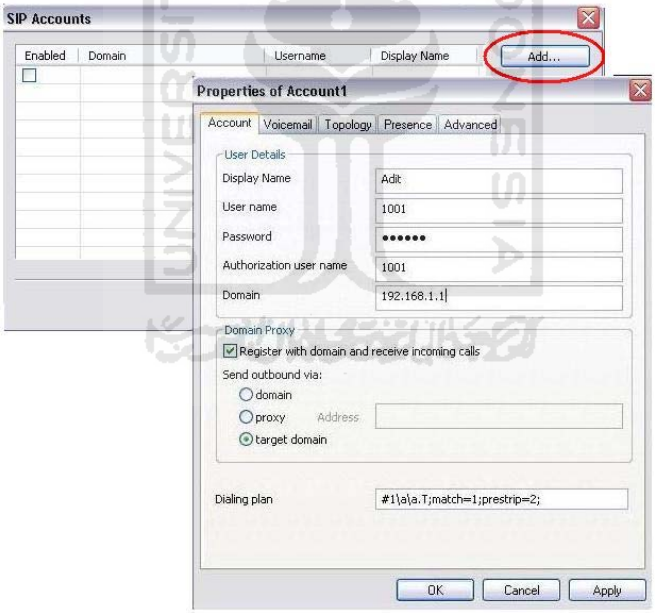


Gambar 3. 10 Pembuatan path directory

6. Konfigurasi Klien

Sistem operasi yang digunakan pada klien adalah windows XP dengan konfigurasi alamat IP yang mengacu pada table 3.1. Konfigurasi selanjutnya yaitu melakukan setting user pada X-LITE, konfigurasi ini digunakan untuk melakukan registrasi klien ke server voip. Untuk lebih jelasnya dapat dilihat pada gambar 3.15 dan gambar 3.16 berikut:

Gambar 3. 11 Interface X-Lite

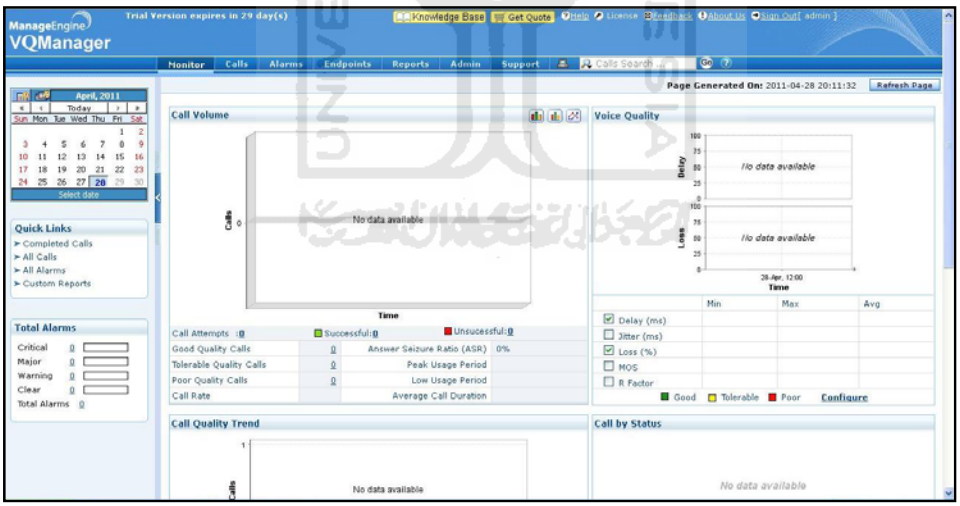


Gambar 3. 12 Konfigurasi klien pada X-Lite

Konfigurasi selanjutnya pada sisi aplikasi VQManager. VQManager berguna untuk monitoring pada voip server. Pada gambar 3.17 menampilkan halaman login pada VQmanager. Username yang digunakan “admin” sedangkan password yang digunakan “admin”.

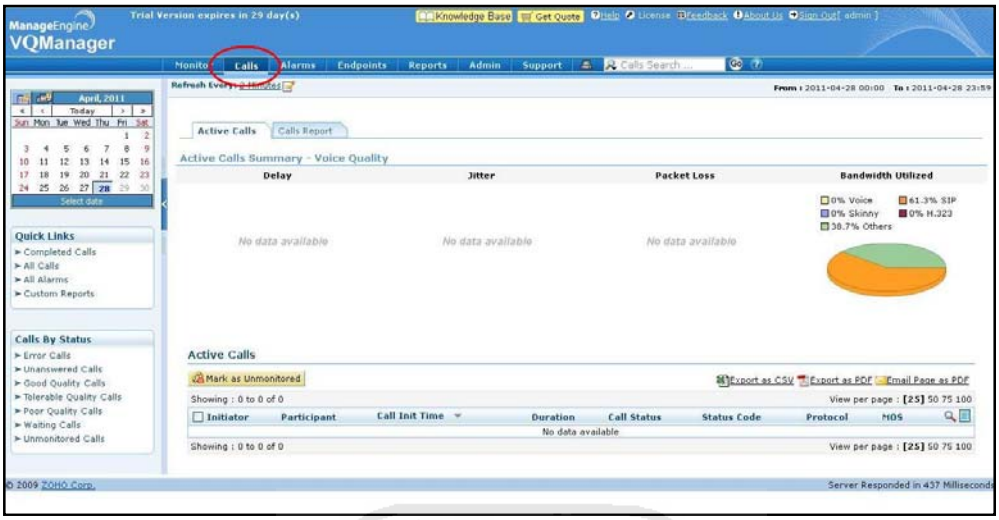
Gambar 3. 13 Tampilan halaman login VQManager

Setelah proses login berhasil akan di redirect atau arahkan langsung kehalaman home. Pada gambar 3.18 akan menampilkan halaman home dari VQManager.



Gambar 3. 14 Tampilah halaman home VQManager

Untuk mendapatkan data delay, jitter, dan paket loss pada proses VOIP dapat dilakukan dengan memilih menu calls ketika adanya komunikasi telepon. Untuk melihat tampilan dapat dilihat pada gambar 3.19 sebagai berikut:.



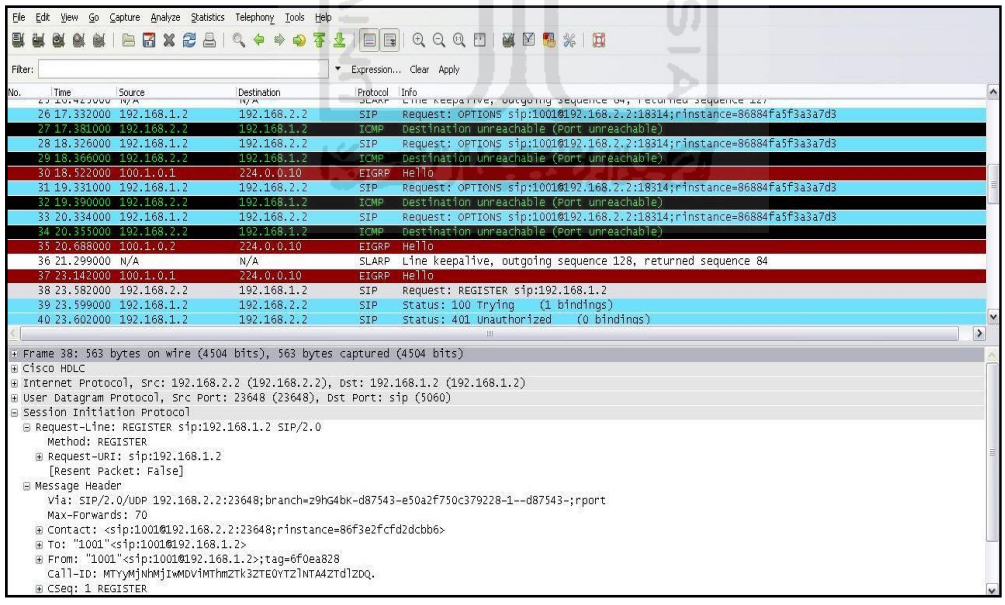
Gambar 3. 15 Tampilan menu calls

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil dan Pembahasan Keamanan

Pengujian keamanan pada penelitian ini menitikberatkan pada perbandingan hasil sebelum dan sesudah implementasi GRE Over IPSec. Metode yang digunakan adalah *sniffing* pada jaringan WAN. Dengan metode *sniffing*, pencurian data dilakukan oleh pihak yang tidak berwenang untuk mendapatkan informasi yang diinginkan.

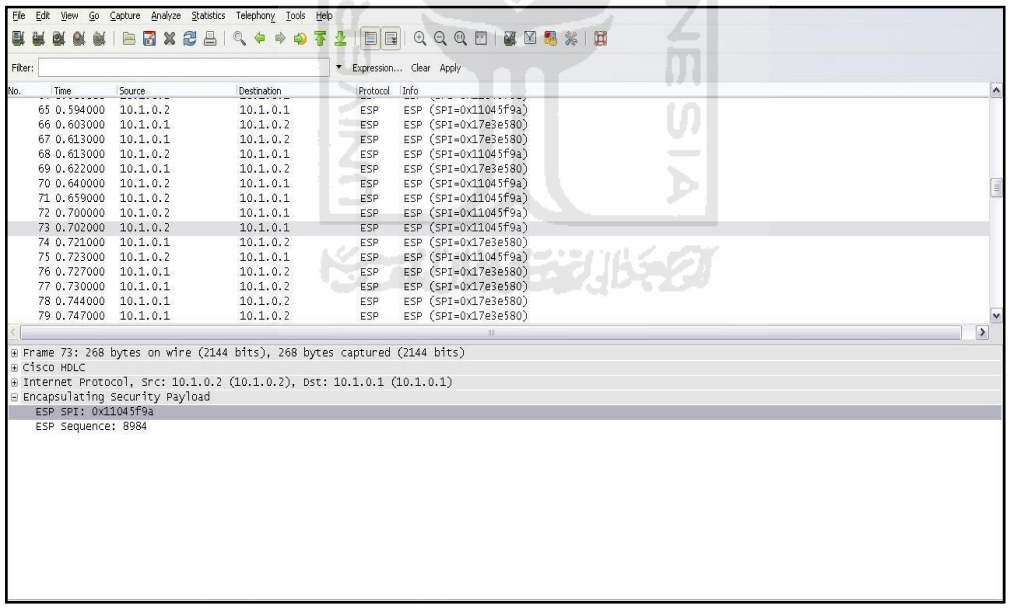
Sniffing dilakukan dengan menggunakan software Wireshark. Wireshark berperan untuk melakukan *snifer* yang menangkap semua paket data yang melewati jaringan WAN. Pada gambar 4.1 menunjukan hasil *sniffing* menggunakan wireshark tanpa implementasi GRE Over IPSec.



Gambar 4. 1 Hasil sniffing tanpa implementasi GRE Over IPSec

Dari gambar 4.1 terlihat bahwa data yang dikirim melalui jaringan WAN dapat diidentifikasi jenis informasi paket data secara jelas tanpa enkripsi. Pada gambar 4.1 terlihat jelas informasi mengenai protokol SIP yang digunakan untuk melakukan registrasi ke server voip baik sumber, tujuan, detail alamatnya. Selain itu ketika user sedang malakukan komunikasi suara, *snifer* dapat merekam dan memutar ulang komunikasi tersebut. Hal ini dapat mengakibatkan komunikasi antara suara user, dapat diketahui oleh pihak yang tidak berwenang. Selain pada proses diatas, sniffing dapat diterapkan pada protokol lainnya seperti telnet, ICMP, layanan WEB, FTP, dan sebagainya.

Hal ini tentu berbeda apabila dibandingkan dengan hasil *sniffing* sesudah pengimplementasian GRE Over IPSec. Pada gambar 4.2 akan menunjukan hasil *sniffing* menggunakan wireshark setelah implementasi GRE Over IPSec.



Gambar 4. 2 Hasil sniffing dengan Implementasi GRE Over IPSec

Gambar 4.2, merupakan hasil capture paket data setelah mengimplementasi GRE Over IPSec. Jika diperhatikan, semua informasi paket terenkripsi dengan protokol ESP. Hal ini dapat mempersulit *sniffer* untuk

mengambil informasi paket data. Dengan adanya enkripsi paket dapat menjamin kerahasiaan paket data yang dikirimkan.

Dengan adanya kedua implementasi diatas, dapat dilihat perbedaan hasil capture sebelum dan sesudah pengaplikasian GRE Over IPSec. Setelah menggunakan GRE Over IPSec, informasi paket data yang dikirimkan terenkripsi oleh protokol ipsec. Sehingga tidak dapat diambil informasi apapun selain alamat sumber, alamat tujuan dan juga protokol ESP yang ditampilkan oleh wireshark. Perbandingan sebelum dan sesudah mengimplementasi GRE Over IPSec dapat dilihat pada table 4.1 berikut:

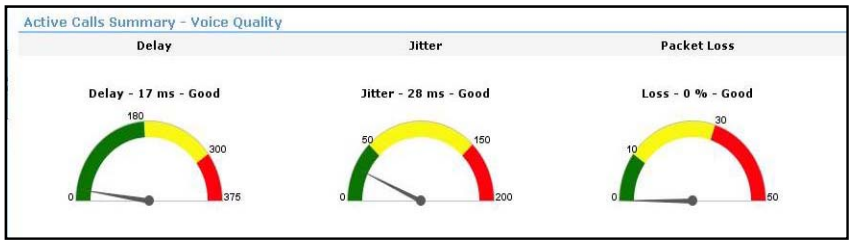
Tabel 4. 1 Perbandingan Keamanan

Parameter	**Tanpa GRE Over IPSec**	**Menggunakan GRE Over IPSec**
1.Protocol	SIP,EGRP,ICMP,SLARP	ESP
2.Voice Recording	Dapat dilakukan	Tidak dapat dilakukan
3.Enkripsi	Tidak terenkripsi	Terenkripsi

4.2 Performa

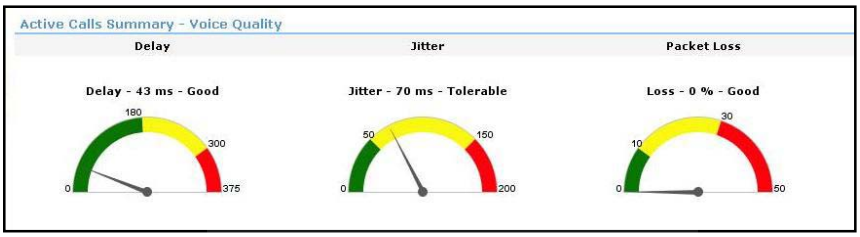
4.2.1 Performa Pada VOIP

Pengujian pada VOIP digunakan sebagai parameter untuk melihat perbedaan performa antara sebelum dan sesudah menggunakan GRE Over IPSec. Pengujian ini menggunakan delay, jitter, dan paket loss sebagain tolak ukur perbedaan tersebut. Gambar 4.3 menunjukan hasil pengujian delay, jitter, dan paket lost pada VOIP sebelum GRE Over IPSec diaplikasikan.



Gambar 4. 3 Hasil Voice Quality tanpa GRE Over IPSec

Pada suatu keaadaan pengujian dengan hasil seperti yang ditunjukkan pada gambar 4.3, terlihat suatu barometer pada VQManager. Keadaan ini akan menghasilkan nilai yang berbeda apabila sesudah pengimplementasian GRE Over IPSec. Gambar 4.4 menunjukan hasil delay, jitter dan paket loss menggunakan GRE Over IPSec.



Gambar 4. 4 Hasil Voice Quality menggunakan GRE Over IPSec

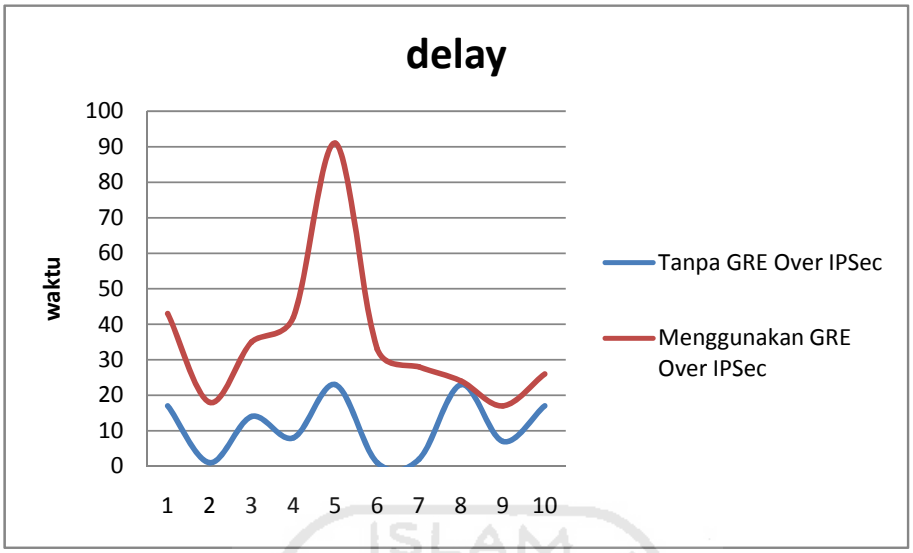
Terdapat perbedaan hasil pengukuran yang sangat jelas ketika sesudah pengimplementasian GRE over IPSec, terjadi peningkatan nilai pada barometer pengukuran dengan VQManager. Penyebab meningkatnya delay dan jitter sesudah penggunaan GRE Over IPSec tersebut disebabkan oleh adanya proses enkripsi pada paket VOIP. Pada percobaan ini dilakukan panggilan telepon sebanyak 10 kali percobaan, baik ketika sebelum maupun sesudah menggunakan GRE Over IPSec. Untuk penjelasan lebih lanjut dapat dilihat dari tabel 4.2 dibawah ini.

Tabel 4. 2 Perbandingan Performa VOIP

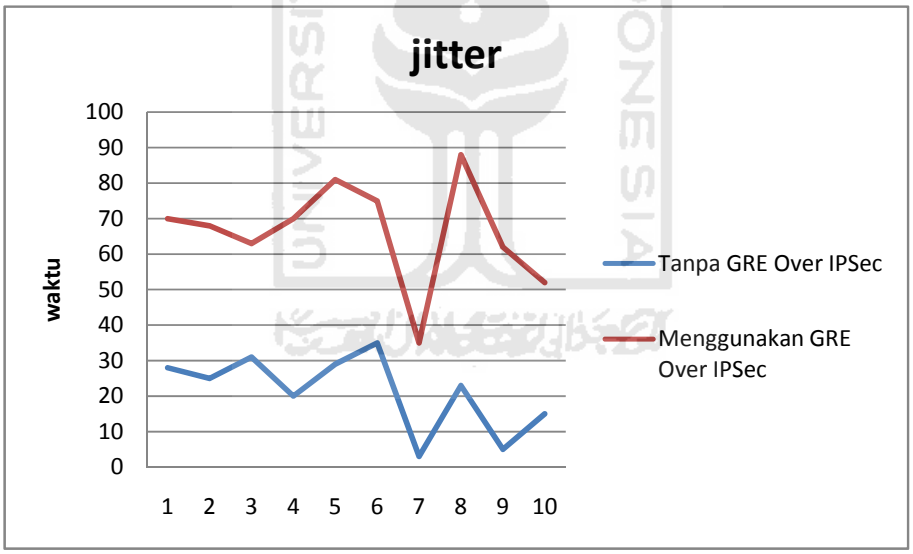
Pengujian	Tanpa GRE Over IPSec			Menggunakan GRE Over IPSec		
	delay (ms)	jitter (ms)	paket loss (ms)	delay (ms)	jitter (ms)	paket loss (ms)
1	17	28	0	43	70	0
2	1	25	0	18	68	0
3	14	31	0	35	63	0
4	8	20	0	42	70	0
5	23	29	0	91	81	0
6	1	35	0	33	75	0
7	2	3	0	28	35	0

Pengujian	Tanpa GRE Over IPSec			Menggunakan GRE Over IPSec		
	delay (ms)	jitter (ms)	paket loss (ms)	delay (ms)	jitter (ms)	paket loss (ms)
8	23	23	0	24	88	0
9	7	5	0	17	62	0
10	17	15	0	26	52	0
Rata-rata	11	21	0	35.7	46.3	0

Perbandingan delay baik sebelum maupun sesudah pengimplemtasian GRE Over IPSec mengalami kenaikan sebesar 215,92%, sedangkan pada jitter mengalami kenaikan sebesar 116,35%. Kenaikan delay dan jitter menyebabkan penurunan performa dari aplikasi VOIP. Berdasarkan table 4.2 dapat dibuat grafik perbandingan delay dan jitter antara sebelum dan sesudah implementasi GRE Over IPSec. Gambar 4.5 menunjukkan grafik perbandingan delay sebelum dan sesudah implementasi GRE Over IPSec, dan gambar 4.6 merupakan grafik perbandingan jitter sebelum dan sesudah implementasi GRE Over IPSec. Sedangkan parameter paket loss baik sebelum maupun sesudah implementasi GRE Over IPSec tidak mengalami perubahan (bernilai 0), maka penggunaan GRE Over IPSec tidak berpengaruh pada parameter paket loss.



Gambar 4. 5 Grafik perbadingan delay

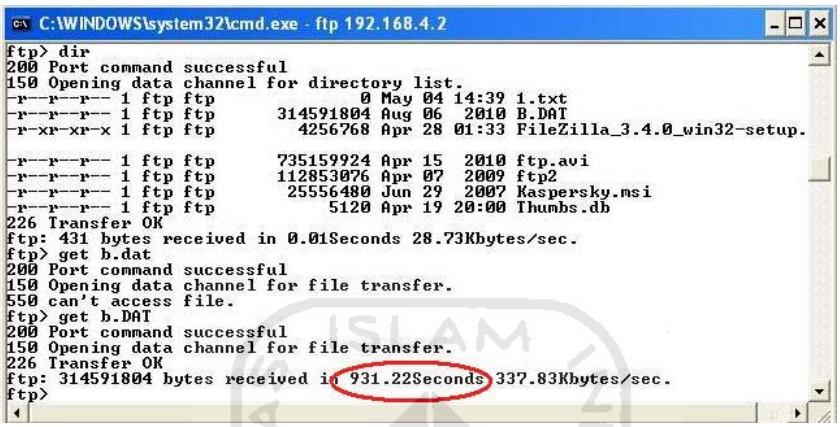


Gambar 4. 6 Grafik perbandingan jitter

4.2.2 Performa FTP

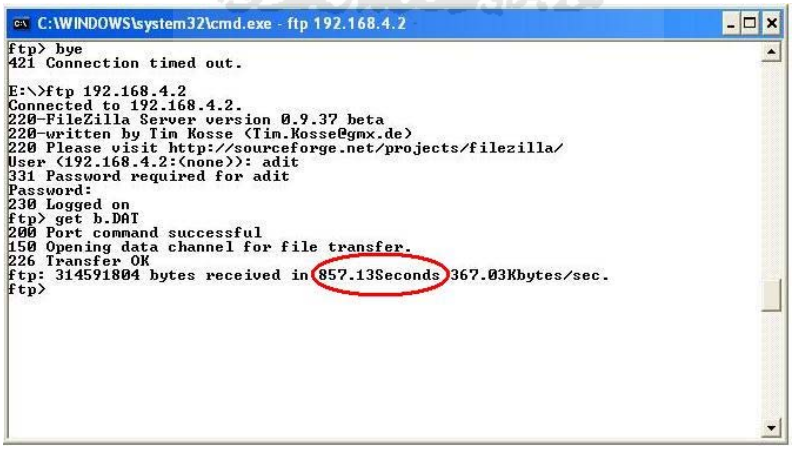
Untuk pengujian performace menggunakan FTP sebelum dan setelah menggunakan GRE Over IPSec, dilakukan dengan membandingkan lama waktu pengiriman data sebesar 300 MB. Pada skenario ini, klien FTP melakukan akses ke server FTP kemudian mengunduh file. Hasil pengujian performa FTP dapat

dilihat pada lama waktu pengiriman file dari server ke klien yang dilakukan sebanyak 6 kali pengiriman data FTP baik sebelum dan sesudah menggunakan GRE Over IPSec. Contoh hasil pengiriman sebelum menggunakan GRE Over IPSec dapat dilihat pada gambar 4.7 berikut:.



Gambar 4. 7 Hasil pengiriman FTP tanpa menggunakan GRE Over IPSec

Berdasarkan gambar 4.7 dapat dilihat lama waktu pengiriman data menggunakan FTP sebelum implementasi GRE Over IPSec sebesar 931.22 detik. Sedangkan untuk hasil pengiriman data menggunakan FTP sesudah pengimplementasian GRE Over IPSec dapat dilihat pada gambar 4.8 berikut:.



Gambar 4. 8 Hasil pengiriman FTP setelah menggunakan GRE Over IPSec

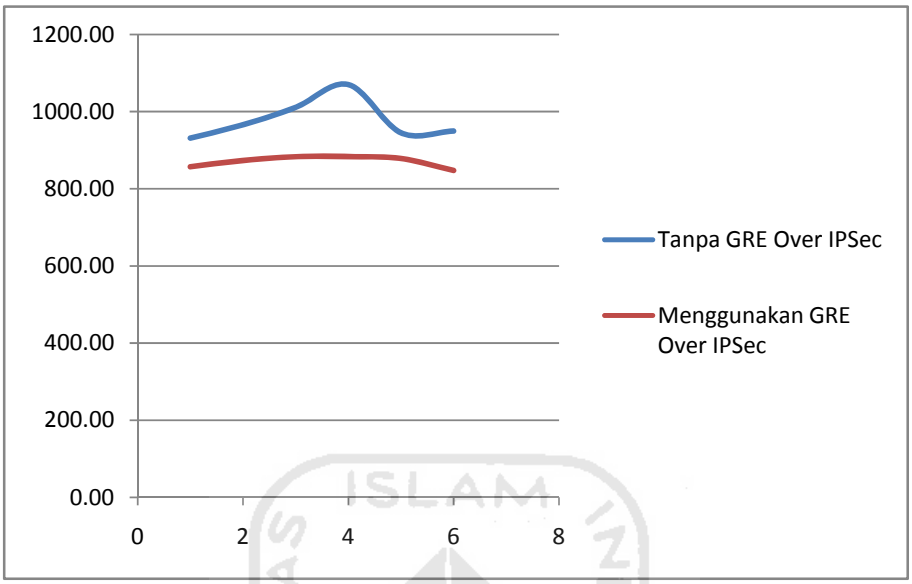
Bedasarkan gambar 4.8, dapat dilihat lama waktu pengiriman data menggunakan GRE Over IPSec sebesar 857.13 detik. Untuk perbandingan hasil pengiriman data menggunakan FTP baik sebelum dan sesudah pengimplementasian GRE Over IPSec terdpat pada table 4.3 berikut:

Tabel 4. 3 Perbandingan Performa FTP

Pengujian	Tanpa GRE Over IPSec	Menggunakan GRE Over IPSec
1	931,22 detik	857,13 detik
2	965,74 detik	873,38 detik
3	1010,80 detik	883,33 detik
4	1070,08 detik	883,33 detik
5	944,98 detik	878,63 detik
6	949,50 detik	847,54 detik
Rata-Rata	978,72 detik	870,56 detik

Dari hasil pengambilan data yang telah dilakukan seperti yang tertera pada Tabel 4.3, terdapat ketidaksesuaian hasil terhadap hepotesa awal. Pada hipotesa awal dimungkinkan adanya penurunan performa pengiriman paket data dengan FTP setelah pengimplementasian GRE Over IPSec. Ketidak sesuaian hasil terhadap hipotesa dimungkinkan karena adanya penurunan ukuran frame pada paket yang dilewatkan. Besarnya ukuran frame sebelum pengimplementasian GRE Over IPSec adalah 1460 bytes, dan setelah pengimplementasian GRE Over IPSec ada lah 1387 bytes menggunakan FTP setelah pengimplementasian GRE Over IPSec. Dengan adanya ketidaksesuain tersebut, perlu dilakukan penelitian lebih lanjut untuk mengetahui faktor yang mempengaruhi hasil seperti yang tertera pada table 4.3 diatas.

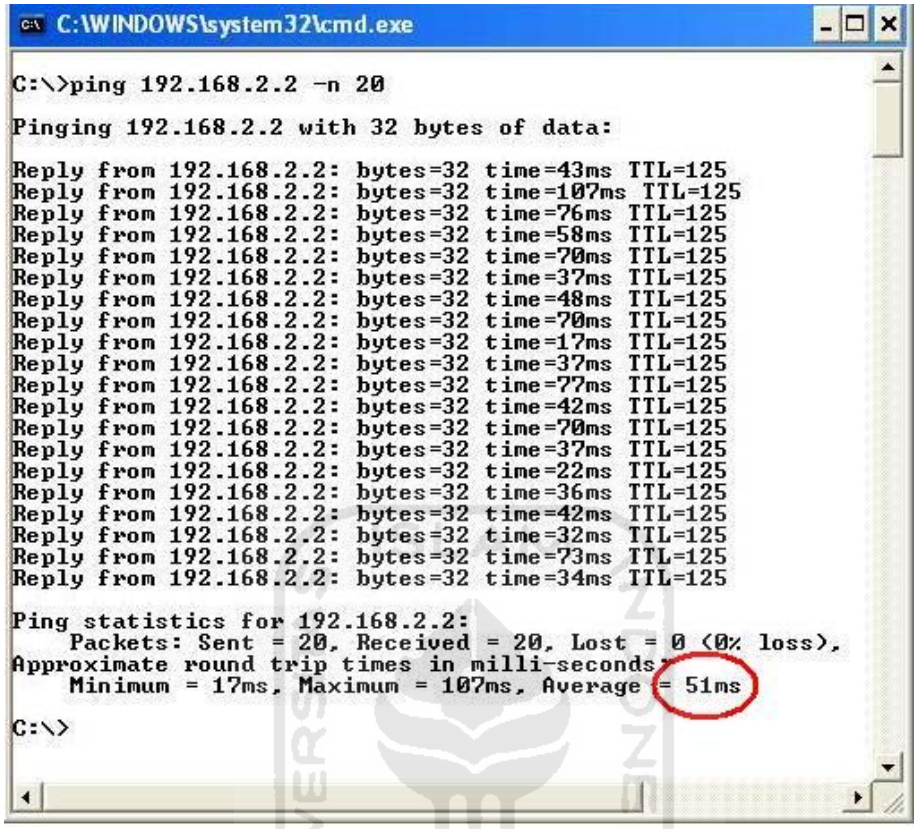
Perbandingan hasil pengiriman data FTP baik sebelum maupun sesudah pengimplementasian GRE Over IPSec mengalami penurunan pada lama waktu pengiriman sebesar 11.05%. Perbandingan lebih lanjut pengiriman paket data dengan FTP baik sebelum maupun sesudah implementasi GRE Over IPSec dapat dijelaskan seperti pada gambar 4.9.



Gambar 4. 9 Grafik Perbadingan FTP

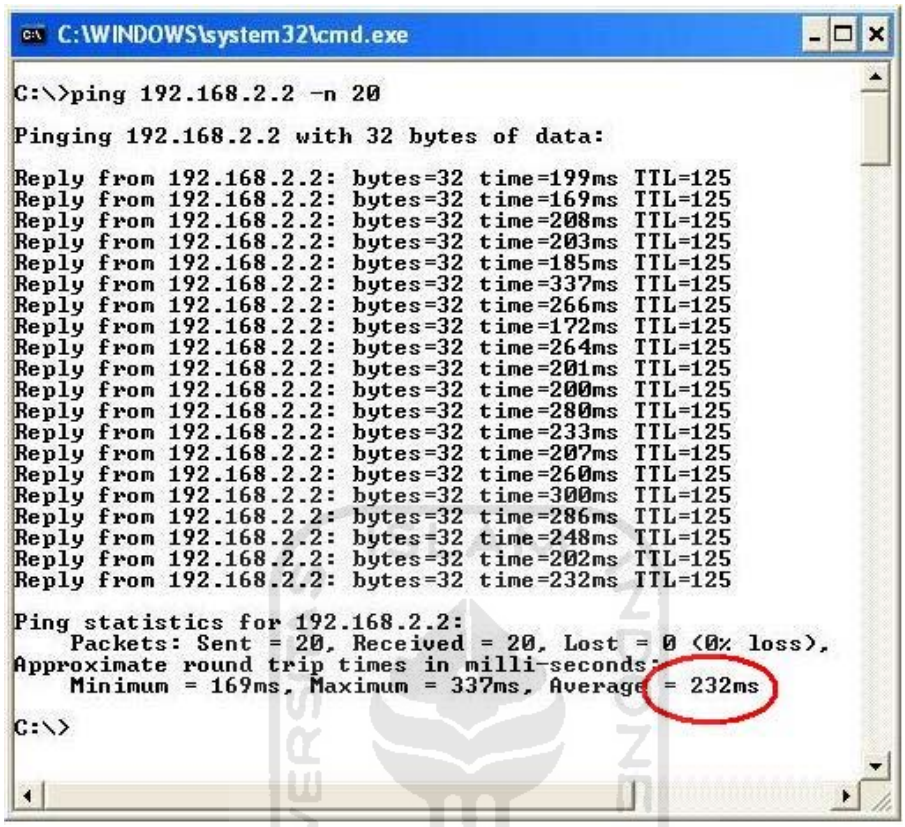
4.2.3 Performa ICMP

Pengukuran parameter untuk melihat perbedaan performa antara sebelum dan sesudah penggunaan GRE Over IPSec, dilanjutkan dengan pengujian ICMP. Pengujian ini dilakukan dengan membandingkan hasil pengujian ICMP menggunakan paket ping dari klien 1 ke klien *2*. Percobaan ini dilakukan sebanyak 10 kali percobaan menggunakan aplikasi ICMP untuk diambil nilai rata-rata secara keseluruhannya. Pada gambar 4.10 menunjukkan hasil ping sebelum menggunakan GRE Over IPSec.



Gambar 4. 10 Ping sebelum menggunakan GRE Over IPSec

Berdasarkan gambar 4.10 dapat dilihat hasil rata-rata waktu pengiriman paket ping sebanyak 20 kali adalah 51ms. Hal ini tentunya berbeda dengan hasil paket data ping ketika menggunakan GRE Over IPSec. Pada gambar 4.11 menampilkan hasil ping menggunakan GRE Over IPSec .



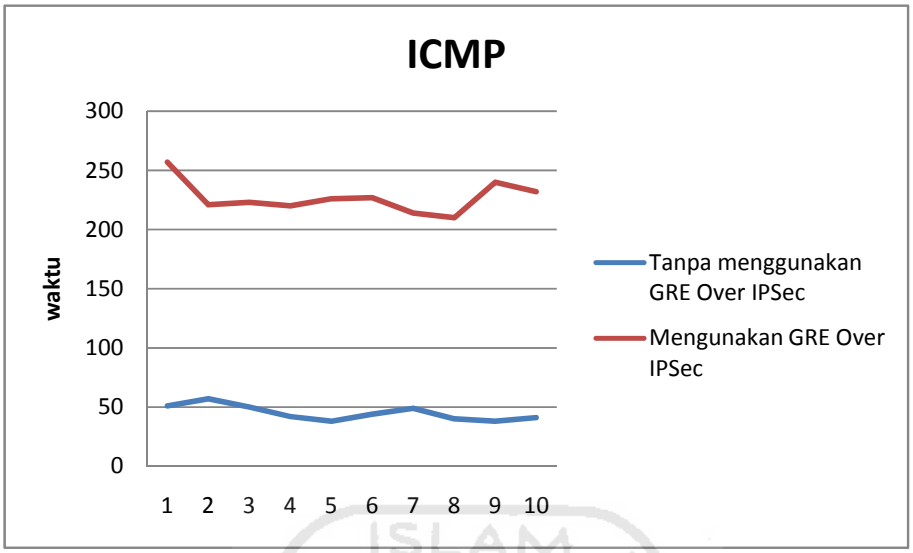
Gambar 4. 11 Ping setelah menggunakan GRE Over IPSec

Dari gambar 4.8 dapat dilihat hasil rata-rata setelah menggunakan GRE Over IPSec adalah 232 ms. Terjadi perbedaan lama waktu pengiriman data seperti yang ditunjukkan pada dua gambar diatas. Pengiriman paket ping setelah pengaplikasian GRE Over IPSec akan membutuhkan waktu yang lebih lama, karena membutuhkan proses enkripsi terlebih dahulu. Untuk lebih jelasnya dapat dilihat dari tabel 4.3 berikut:.

Tabel 4. 4 Perbandingan Peforma ICMP

Pengujian	Tanpa GRE Over IPSEC	Menggunakan GRE Over IPSec
1	51 ms	257 ms
2	57 ms	221 ms
3	50 ms	223 ms
4	42 ms	220 ms
5	38 ms	226 ms
6	44 ms	227 ms
7	49 ms	214 ms
8	40 ms	210 ms
9	38 ms	240 ms
10	41ms	232 ms
Rata-rata	45 ms	227 ms

Perubahan data ICMP baik sebelum maupun sesudah pengimplemtasian GRE Over IPSec naik sebesar 404.44%, hal ini menyebabkan menurunnya performa pada aplikasi ICMP Berdasarkan table 4.4 perbandingan waktu pengiriman paket ping baik sebelum dan sesudah pengimplementasian GRE Over IPSec dapat dibuat sebuah grafik yang menunjukkan perbedaan perbandingan waktu. Gambar 4.12 menunjukan grafik perbandingan sebagai berikut:.



Gambar 4. 12 Grafik perbandingan ICMP

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan implementasi dan pengujian, dapat diambil kesimpulan sebagai berikut:.

1. Implementasi GRE Over IPSec memberikan solosi pada kemanan tetapi dapat memungkinkan menurunkan performa pada aplikasi jaringan.
2. Implementasi GRE Over IPSec dapat menurunkan kinerja VOIP, hal tersebut terlihat pada peningkatan nilai rata-rata delay sebesar 215.92% dan jitter sebesar 116.35%. Sedangkan pada paket loss tidak mengalami perubahan.
3. Implementasi GRE Over IPSec dapat menurunkan kinerja ICMP , hal ini dapat terlihat pada peningkatan nilai rata-rata pada lama waktu pengiriman data sebesar 404,44%.
4. Implementasi GRE Over IPSec dimungkinkan terjadinya kenaikan performa FTP, hal ini dapat terlihat pada penurunan nilai rata-rata pada lama waktu pengiriman data sebesar 11.05%.
5. Implementasi GRE Over IPSec dapat menjadi solusi karena terbukti mampu menjalankan fungsi *tunnel* secara optimal dan keamanan data terlindungi.

5.2 Saran

Dibutuhkan penelitian lebih lanjut pada implementasi FTP menggunakan GRE Over IPSec, karena terdapat hasil yang tidak sesuai dengan hipotesa awal yaitu keamanan data pada GRE Over IPSec berbanding terbalik dengan tingkat performa.

DAFTAR PUSTAKA

[CISCO] Cisco System "GRE Over IPSEC" http://www.cisco.com diakses pada tanggal 10 januari 2011.

[FAR84] D. Farinacci "Generic Routing Encapsulation (GRE)" http://tools.ietf.org/html/rfc2784 diakses pada tanggal 30 januari 2011.

[HAN01] S. Hanks and Network Working Group " Generic Routing Encapsulation (GRE)" http://tools.ietf.org/html/rfc1701 diakses pada tanggal 25 desember 2011.

[MHS11] Sanny, Muhammad R "KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN)" http://www.cert.or.id/~budi/courses/ec5010/projects/rusdy-report.doc diakses pada tanggal 30 mei 2011

[MRS41] Mircrosoft Corp. "VPN Tunnels - GRE Protocol 47 Packet Description and Use" http://support.microsoft.com/kb/241251 diakses pada tanggal 5 april 2011.

[NKC10] Nemo, "*Fun With the IP Security Protocol*". Diakses dari http://www.kecoak-elektronik.net pada tanggal 10 januari 2011.

[OWP11] Purbo, Onno W “Virtual Private Network (VPN) sebagai alternatif Komunikasi Data Pada Jaringan Skala Luas (WAN)”http://kambing.ui.ac.id/onnopurbo/library/library-ref-ind/ref-ind-3/network/VPN_jurnal.pdf diakses pada tanggal 30 mei 201

[POS11] J. Postel and Network Working Group “FILE TRANSFER PROTOCOL (FTP)” http://www.faqs.org/rfcs/rfc959.html diakses pada tanggal 31 mei 2011

[SHP00] Pakpahan, Suhardi “JARINGAN WORKGROUP, LAN & WAN” http://onno.vlsm.org/v11/ref-ind-1/network/jaringan-workgroup-lan-wan-1998.rtf diakses pada tanggal 30 mei 2011