Penggunaan Virtual Private Network Untuk Pengamanan Komunikasi Pada VoIP

Joko Triwanto[1] dan Eko Apri Setiawan[1]

ABSTRACT: *Along with the growth of computer network that quicker enable for past the voice traffic through computer network or usually called VoIP (Voice Over Internet Protocol). The VoIP user was opinioned as one of the cheap alternative technology with capability facilities such as line extention, Video call, VoIP to PSTN call, PSTN to VoIP call, and digital receptionist (IVR). But the weakness of VoIP system is the security of VoIP call that could buged so that the voice communication could recorded and the privacy did't guaranteed. To solve this weakness VoIP communication use VPN were done by using fast, easy and cheap. The security development stake procces in this VoIP system consist of stake, configuration, and examination. This security examination valued with voice communication can't buged that means the user VoIP privacy more guarantee.*
KEYWORDS: *Voice over Internet Protocol, Virtual Private Network, IPv4, VoIP over VPN*

ABSTRAK: Berkembangnya teknologi sekarang ini memacu untuk membuat teknologi yang semakin murah atau terjangkau. Seiring berkembangnya jaringan komputer yang semakin pesat memungkinkan untuk melewatkan trafik suara melalui jaringan komputer atau biasa yang disebut VoIP (Voice Over Internet Protocol). Penggunaan VoIP dianggap sebagai salah satu teknologi alternatif yang murah dengan kemampuan memberikan layanan seperti *line extension*, *Video Call*, panggilan VoIP to PSTN panggilan PSTN to VoIP, serta digital receptionist (IVR). Namun kelemahan dari sistem *VoIP* disini adalah keamanan panggilan VoIP yang bisa dilakukan penyadapan sehingga komunikasi suara dapat terekam dan privasi tidak terjamin. Untuk mengatasi kelemahan ini pelewatan komunikasi VoIP dilakukan dengan menggunakan VPN secara cepat, mudah dan murah. Proses rancang bangun security pada sistem VoIP ini terdiri dari perancangan, konfigurasi dan pengujian. Pengujian *security* ini dinilai dengan komunikasi suara tidak dapat disadap yang berarti privasi dari pengguna VoIP ini terjamin.
KATA KUNCI: *Voice over Internet Protocol, Virtual Private Network, IPv4, VoIP over VPN*

PENDAHULUAN

Seiring pesatnya perkembangan jumlah komputer yang saling terhubung dengan lainnya dan yang biasa disebut dengan jaringan komputer. Teknologi yang saling menghubungkan komputer di dunia memungkinkan untuk dapat saling bertukar informasi dan data, bahkan dapat saling berkomunikasi dan bertukar informasi berupa gambar atau video . Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewatkan trafik suara melalui jaringan komputer atau biasa yang disebut VoIP (Voice Over Internet Protocol). VoIP adalah teknologi yang menawarkan telepon melalui jaringan IP (Internet Protocol) dengan terknologi ini mengubah suara menjadi kode digital melalui jaringan paket-paket data, bukan sirkuit analog telepon biasa. Penggunaan jaringan IP memungkinkan penekanan biaya dikarenakan tidak perlu membangun sebuah infrastruktur baru untuk komunikasi suara dan penggunaan lebar data (bandwidth) yang lebih kecil dibandingkan telepon biasa.

Penggunaan teknologi VoIP yang lebih efisien akan semakin dipermudah karena dapat digabungkan dengan jaringan telepon lokal yang sudah ada, dengan menggunakan VoIP gateway yang akan disambungkan dengan PABX. Setiap individu dapat membangun dan mengembangkan infrastrukturnya secara mandiri, dikarenakan penggunaan sistem operasi berbasis linux / open source Trixbox yang memang dikhususkan untuk menangani VoIP.Penggunaan teknologi VoIP jelas menguntungkan bagi penggunanya. Namun , penggunaan komunikasi yang murah dari sisi keamanan kurang begitu di perhatikan. Oleh karena itu keamanan ketika melakukan komunikasi suara merupakan sesuatu yang sangat penting , karena menyangkut privasi penggunanya. Penggunaan VPN (Virtual Private Network) merupakan salah satu alternatif pelewatan komunikasi suara , yang bersifat private atau aman , karena penggunaan koneksi yang telah terenkripsi serta penggunaan private keys, certificate, atau username/password untuk melakukan authentikasi dalam membangun koneksi.

Perumusan Masalah

Berdasarkan latar belakang penyusunan proyek akhir yang telah diuraikan sebelumnya, permasalahan yang dihadapi dirumuskan sebagai berikut:

1) Bagaimana membuat VoIP untuk keperluan komunikasi?
2) Bagaimana meningkatkan keamanan VoIP untuk menjaga data komunikasi?

Tujuan

Tujuan pada proyek ini adalah :

1) Mengimplementasikan Asterisk sebagai VoIP *server* untuk komunikasi antara mahasiswa dan juga dosen ataupu satu sama lainnya.
2) Mengimplementasikan VoIP *over* VPN yang dapat membantu dalam meningkatkan keamanan data pada *VoIP*.

[1] Jurusan Teknik Informatika Perguruan Tinggi Raharja Tangerang Banten

TINJAUAN PUSTAKA

VoIP

Voice over Internet Protocol (VoIP) adalah teknologi yang memungkinkan membuat panggilan telepon dengan menggunakan koneksi internet *broadband*, bukan telepon biasa[1]. Pada dasarnya, individu sekarang dapat menggunakan koneksi internet *broadband* mereka untuk menempatkan panggilan telepon daripada menggunakan saluran telepon tradisional mereka. Idealnya, kualitas suara adalah sama dengan jalur telepon standar dan oleh karena itu orang-orang di ujung telepon tidak akan pernah tahu perbedaan. Teknologi, walaupun kompleks, cukup langsung.VoIP selular yang mengambil teratur, percakapan suara analog dan mengkonversikannya ke dalam data yang kemudian dapat dikirim melalui Internet menggunakan kecepatan tinggi koneksi *broadband*. Di ujung lain dari panggilan, data tersebut akan diubah kembali menjadi sinyal analog yang sistem telepon konvensional dapat memberikan kepada orang yang jumlah awalnya menelepon. Semua ini dicapai dengan mulus ketika menggunakan telepon biasa pada kedua ujungnya. Dengan kata lain, orang tidak perlu berbicara melalui mikrofon komputer mereka untuk mendapatkan hasil maksimal dari layanan VoIP. Menelepon dengan menggunakan VoIP banyak keuntungannya, diantaranya adalah dari segi biaya jela lebih murah dari tarif telepon tradisional, karena jaringan IP bersifat global.

VPN

VPN adalah singkatan dari *virtual private network*, yaitu jaringan pribadi (lokal) yang menggunakan media nonpribadi (publik/*internet*) untuk menghubungkan antar *remote-site* secara aman[2]. Perlu penerapan teknologi tertentu yang menggunakan media yang umum, tetapi *traffic* (lalu lintas) jalur data yang dikirim antar remote-site tidak dapat di-*snifing* (disadap) dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya.

IP Address

Alamat IP (*Internet Protocol Address* atau sering disingkat IP) adalah deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan Internet[9][8]. Panjang dari angka ini adalah 32-bit (untuk IPv4 / IP versi 4), dan 128-bit (untuk IPv6 / IP versi 6) yang menunjukan alamat dari komputer tersebut pada jaringan internet berbasis TCP/IP.

1. Asterisk

Asterisk adalah *tools open source* yang sangat popular untuk teknologi komunikasi. Asterisk membuat teknologi komunikasi menjadi mudah untuk dibuat dan dikembangkan pada sebuah aplikasi telepon jarak jauh.Asterisk dirilis sebagai open source di bawah GNU General Public License(GPL) dan tersedia untuk di-*download* secara gratis. Asterisk juga merupakan kunci pada pertumbuhan teknologi VoIP.

Open VPN

OpenVPN adalah sebuah implementasi VPN *open source* yang menggunakan enkripsi SSL. Implementasi *user* OpenVPN tersedia untuk banyak sistem operasi, termasuk Linux, Windows 2000/XP atau yang lebih tinggi, OpenBSD, FreeBSD, NetBSD, Mac OS X, dan Solaris. Pada sebuah VPN, dia akan meng-enkapsulasi semua trafik (termasuk protokol DNS dan protokol-protokol lain) di tunnel yang terenkripsi, jadi bukan hanya satu port TCP saja. Kebanyakan orang merasa hal itu sangat memudahkan untuk dimengerti dan diatur daripada IPSEC.

Ubuntu

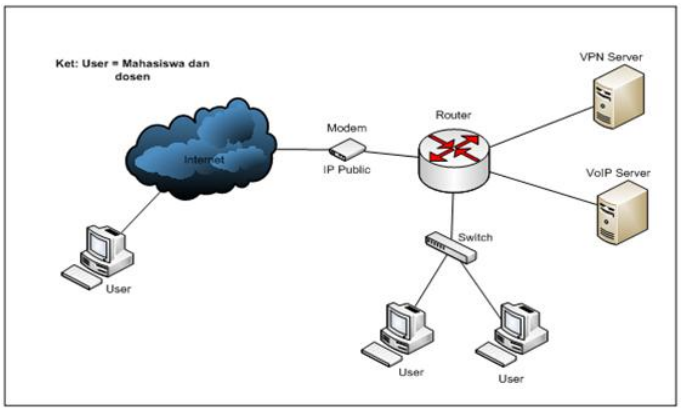
Ubuntu merupakan salah satu distribusi Linux yang berbasiskan Debian. Proyek Ubuntu resmi disponsori oleh Canonical Ltd yang merupakan perusahaan milik seorang kosmonot asal Afrika Selatan Mark Shuttleworth. Nama Ubuntu diambil dari nama sebuah konsep ideologi di Afrika Selatan, "Ubuntu" berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Filosofi Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

WireShark

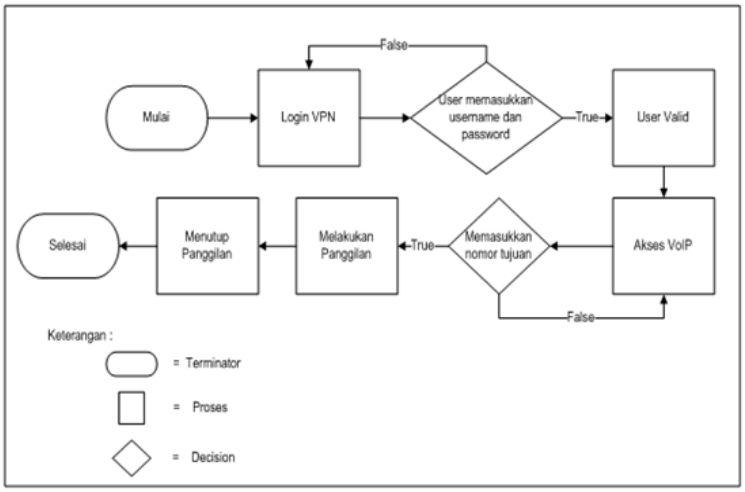
WireShark adalah satu dari sekian banyak *tool Network Analyzer* yang dipakai oleh orang – orang yang bekerja di bidang jaringan yang ingin melihat atau menganalisa paket jaringan, pengembangan protokol jaringan serta edukasi bagi yang ingin memperdalam ilmu nya dalam jaringan komputer. Yang menjadi kelebihan bagi wireshark adalah lisensi nya yang free alias open source. Tentu hal ini sangat menarik minat orang untuk menggunakan aplikasi ini bagi pekerjaan di bidang jaringan. Selain itu Wireshark juga dibuat dengan berbasiskan GUI yang cukup baik dan bagus.

PEMBAHASAN

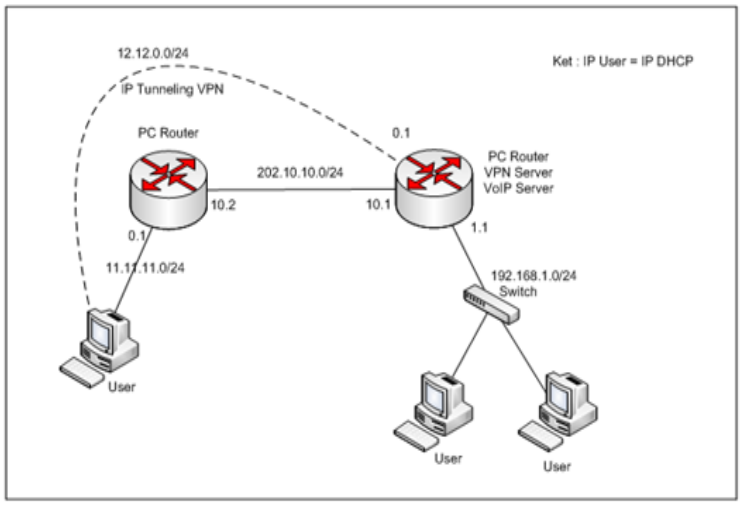
Pada proyek ini akan dibuat sistem untuk berkomunikasi secara aman dari sisi penyadapan dan juga menghemat dalam kendala biaya yang selalu dialami dalam berkomunikasi. Maka dari itu penulis mencoba membangun VoIP *over* VPN, yaitu dengan membangun VoIP yang merupakan sistem komunikasi dengan melalui jalur VPN yang memberikan keamanan dan integritas data serta fungsionalitas yang mendukung untuk mengamankan jalur komunikasi suara pada VoIP. Berikut adalah perancangan dan desain sistem serta flowchart VoIP:



■ **Gambar** 1. Skema Perancangan Sistem



■ **Gambar** 2. *Flowchart* Sistem VoIP



■ **Gambar** 3. Desain *Prototype* VoIP *over* VPN

1. Konfigurasi *Server*

Tahapan – tahapan dalam membangun VoIP *over* VPN menggunakan IPv4, mengimplementasikan VoIP *over* VPN, dan menguji kemanan komunikasi suara pada VoIP menggunakan *tools* WireShark.

a. Konfigurasi DHCP *Server* dan *Interface* pada Router VPN

DHCP *server* berfungsi untuk memberikan alamat IP kepada *user* tanpa perlu *user* tersebut memasukkan alamat IP secara manual. Pada bagian ini akan dilakukan pengkonfigurasian untuk router yang berfungsi sebagai Router VPN.

b. Konfigurasi DHCP *Server* dan *Interface* pada Router Eksternal

Pada konfigurasi DHCP *Server* dan *Interface* pada Router eksternal tidak terlalu jauh beda pada pengkonfigurasian router VPN hanya saja bedanya pada bagian peroutingan, yaitu router eksternal tidak dilakukan peroutingan agar dibuat senyata mungkin seperti jaringan internet yang sesungguhnya.

c. Konfigurasi *Server* VoIP pada Router VPN

Pada tahap ini *server* VoIP menggunakan platform asterisk yang berbasiskan *Open Source* dan melakukan konfigurasi terhadap dialplan yang terdapat pada asterisk *server* agar *user* dapat berkomunikasi.

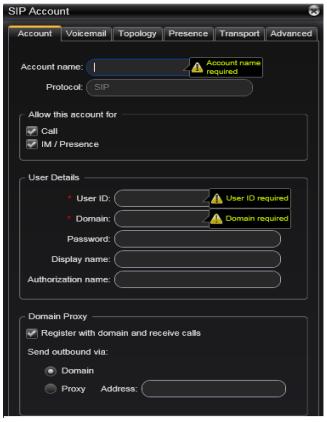
d. Konfigurasi VPN *Server* pada Router VPN

Pada tahap ini dilakukan pengkonfigurasian terhadap layanan VPN menggunakan OpenVPN.

e. Konfigurasi *User* VoIP

Pada tahap ini dilakukan konfigurasi pada *user* VoIP dengan tahapan sebagai berikut :

1) Unduh dan install x-lite softphone versi 4.1 dari website x-lite.
2) Konfigurasi *user* dengan menggunakan *user* ID dan password telah terdaftar pada asterisk, dan mengisi domain yang berisi IP publik *server* VoIP.



■ **Gambar** 4. Login X-Lite Softphone

f. Konfigurasi VPN *user*

Pada tahap ini dilakukan konfigurasi bagi *user* VPN dengan beberapa tahapan antara lain :

1) Instalasi VPN klien dengan mengunduh dari website VPN untuk platform windows.
2) Copy file client.ovpn yang terdapat pada folder sample-config ke dalam folder config.
3) Copy file ca.crt, client.crt, client.key dan dh1024.pem yang telah dibuat pada VPN *server* ke dalam folder config pada PC *user*.
4) Konfigurasi client.ovpn dengan menggunakan *notepad.*

Implementasi VoIP *over* VPN

Pada tahap pengimplementasian dibuat komunikasi VoIP dengan melalui VPN agar lebih mengamankan data suara pada komunikasi tersebut dari serangan penyadapan. Berikut adalah tahapan – tahapan dalam pengimplementasiannya, yaitu :

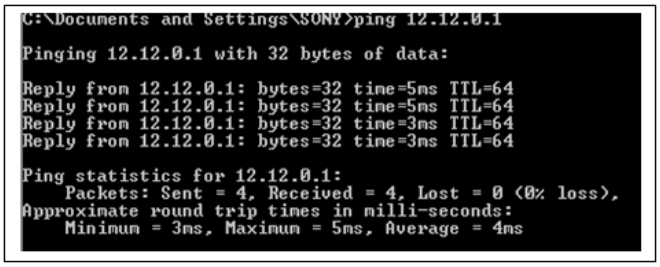
1. Koneksikan *user* eksternal melalui Gui Open VPN client yang telah terpasang pada PC *user* eksternal. Klik kanan pada icon Open VPN yang terletak pada taskbar dan pilih connect. Sebelum itu apabila *user* eksternal ingin memberikan PIN sebagai syarat login dengan menggunakan PC nya itu maka dapat menggunakan pada *icon* VPN dengan mengklik kanan pilih "*Change Password*" dan masukkan PIN yang ingin digunakan.
2. Apabila *user* eksternal ingin Login ke dalam jaringan VPN agar dapat berkomunikasi ke jaringan internal maka, terlebih dahulu memasukkan *User*name dan *Password* yang telah dimilikinya dengan mengklik kanan, kemudian pilih "*connect*".

■ **Gambar** 5. Login Open VPN

3. Setelah *user* eksternal berhasil Login maka dia akan mendapatkan IP *tunneling* klien *Open* VPN.

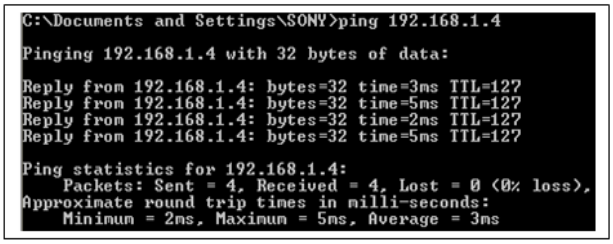
■ **Gambar** 6. IP tunneling Open VPN *user* eksternal

4. Lakukan pengetesan koneksi pada *user* eksternal dengan beberapa bagian, yaitu :
   a. Ping *user* eksternal ke IP VPN s*erver*



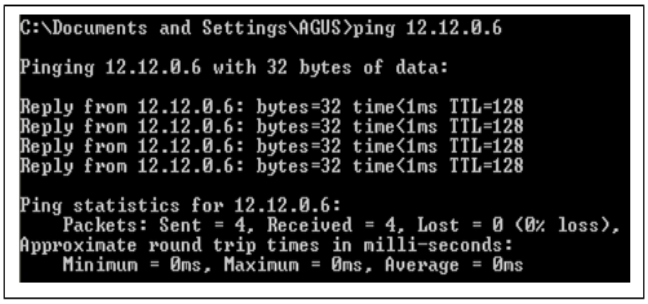
■ **Gambar** 7. Ping *user* eksternal ke IP *server* VPN

   b. Ping *user* eksternal ke IP *user* internal



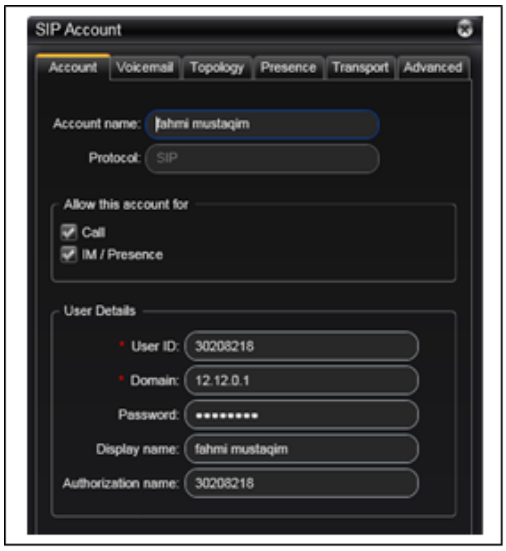
■ **Gambar** 8. Ping *user* eksternal ke IP *user* internal

5. Lakukan juga pengetesan koneksi dari *user* internal ke *user* eksternal dengan menggunakan IP VPN *tunneling.*



■ **Gambar** 9. Ping *user*Internal ke IP VPN *user* eksternal

6. Kemudian setelah selesai melakukan tes koneksi lakukan konfigurasi pada X – Lite di masing – masing *user* internal dan eksternal dan isi domain menggunakan IP *server* VPN sebagai jalur komunikasi yang akan dipakai untuk melakukan panggilan bukan menggunakan IP public yang sebelumnya digunakan.



■ **Gambar** 10. VoIP dengan menggunakan domain IP VPN *server*

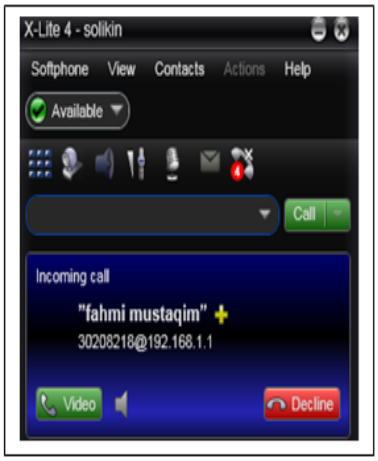
Dan gambar dibawah ini ketika VoIP telah menggunakan IP VPN *server* tapi belum terkoneksi ke Open VPN s*erver*.

■ **Gambar** 11. VoIP dengan domain VPN tapi tidak terhubung ke jalur VPN

7. Lakukan Panggilan pada X-lite dengan contoh *user* eksternal melakukan panggilan ke *user* internal.
   a. *User* eksternal melakukan panggilan ke *user* internal

■ **Gambar** 12. *User* eksternal melakukan panggilan ke *user* internal

   b. *User* internal menerima panggilan *user* eksternal



■ **Gambar** 13. *User* internal menerima panggilan dari *user* eksternal

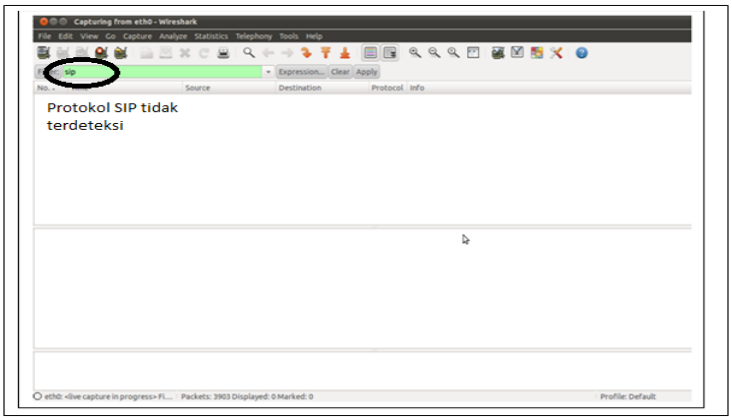
PENGUJIAN

Pada tahap ini akan dilakukan pengujian dari implementasi yang telah dilakukan pada percobaan diatas. Pengujian ini menggunakan *tool Sniffing* yaitu *WireShark* untuk menyadap pada paket – paket data komunikasi VoIP. Berikut adalah pengujian yang akan dilakukan:

a. Pertama koneksikan masing – masing *user* agar terhubung ke PC router VPN dan PC router eksternal.
b. Lakukan pengetesan terhadap koneksi dengan menggunakan ping ke IP public internal.
c. Kemudian lakukan login VPN bagi *user* eksternal dengan menggunakan GUI klien open VPN.
d. Melakukan uji koneksi kembali dengan mengetes ping antara *user* internal dan *user* eksternal.
e. Konfigurasi domain x-lite dengan mengganti menjadi IP VPN *server*.
f. Nyalakan applikasi wireshark.
g. Amati protokol Asterisk yaitu protokol SIP dan lihat komunikasi yang terjadi.
h. Lakukan penyadapan pada komunikasi yang terjadi antara *user* internal dan *user* eksternal

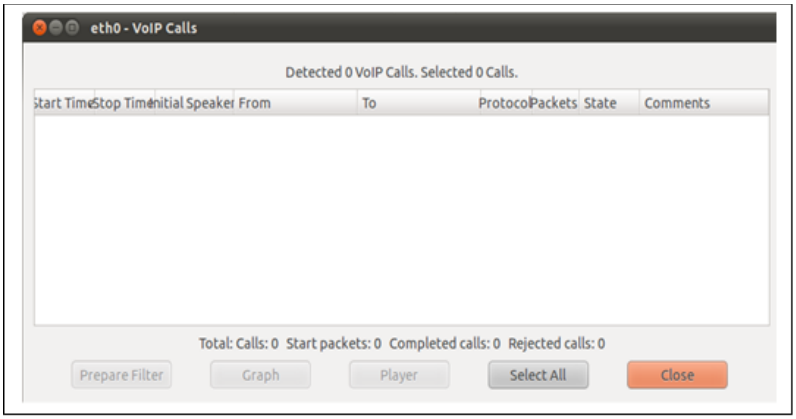
Berikut adalah gambar-gambar hasil penyadapan yang terjadi pada VoIP menggunakan VPN, yaitu :

a. Mengamati jalur protokol SIP.



■ **Gambar** 14. Jalur Protokol SIP setelah VoIP *over* VPN

b. Mengamati data komunikasi VoIP.



■ **Gambar** 15. Komunikasi data panggilan VoIP *over* VPN

Pada kedua tahap pengujian ternyata pada pengujian pertama yang berupa VoIP yang tidak melewati jalur VPN dapat dengan mudah dilakukan penyadapan mulai dari protokol VoIP yaitu SIP, data komunikasi yang sedang melakukan panggilan baik itu berupa asal *user* yang melakukan panggilan dan tujuan panggilan tersebut, grafik panggilan yang terjadi, sampai pada bagian terjadinya penyadapan yang memungkinkan seorang penyadap dapat mendengar komunikasi yang terjadi dari *user* internal dan *user* eksternal. Dari semua hasil yang didapat apabila *server* VoIP dibuat tanpa melalui jalur yang aman tentu saja akan membuat kenyamanan dalam penggunaan VoIP sebagai pengganti telpon tradisional menjadi sangat tidak nyaman karena adanya situasi di saat terjadinya penyadapan dan tujuan panggilan.Akan tetapi pada percobaan kedua dengan membuat VoIP melewati jalur VPN (VoIP *over* VPN) dapat dilihat bahwa protokol VoIP yaitu SIP tidak dapat dilihat traffic yang sedang melakukan panggilan, dan juga data panggilan komunikasi antar *user* tidak akan bisa dilakukan penyadapan. Maka dari itudengan membuat VoIP melalui jalur VPN bisa memberikan kenyamanan bagi pengguna layanan VoIP, karena dalam pembuatannya, VPN terdapat SSL yang dibuat pada saat awal pembuatan VPN berupa certificate Authority (CA), dan pembuatan certificate dan key bagi *user* maupun *server*. Pada VPN juga terdapat metoda Diffle-Hellman sebagai key exchanger dalam pembuatannya.

KESIMPULAN

Kesimpulan dari pengujian dan analisa pada proyek ini adalah :

1. Komunikasi VoIP melalui VPN (VoIP *over* VPN) terbukti aman dari bentuk penyadapan suara (sniffing), hal ini dibuktikan dari hasil pengujian dan analisa jalur komunikasi VoIP *over* VPN secara lokal yang menunjukan bahwa komunikasi suara yang terjadi pada VoIP tidak bisa dilakukan penyadapan atau didengarkan pembicaraan yang terjadi oleh orang yang tidak berkepentingan. VoIP *over* VPN yang menggunakan Open VPN yang merupakan VPN dengan teknologi tunneling dan enskripsi yang melindungi jalur komunikasi VoIP.
2. Implementasi VoIP tanpa menggunakan VPN terbukti rentan dari ancaman penyadapan yang dapat merugikan *user* yang melakukan panggilan.

DAFTAR PUSTAKA

[1] Desantis, M. (2008). *Understanding Voice over Internet Protocol (VoIP).* Retrieved November 27, 2011, from http://www.us-cert.gov/reading_room/understanding_voip.pdf.

[2] Fergusson, P. (1998). *What is a VPN?* Retrieved November 27, 2011, from http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf.

[3] Madcoms. (2010). *Sistem Jaringan.* Yogyakarta: Andi.

[4] Raharja, A. (2006). *Membangun layanan VoIP dengan murah.* Retrieved November 24, 2011, from http://voiprakyat.or.id/data/files/open_voip.pdf.

[5] Raharja, A. (2006). *Session Initiation Protocol.* Retrieved November 24, 2011, from http://www.ilmukomputer.org/wp-content/uploads/2006/08/materi-sip.pdf.

[6] Roddis, S. (2010). *OpenVPN: Easy and Secure Setup Guide.* Retrieved November 27, 2011, from http://www.stevenroddis.com/documents/OpenVPN_Easy_and_Secure_Setup_Guide.pdf.

[7] Safyan, A. (2000). *Server Linux.* Jakarta : Nurul Fikri Computer & statistics, Yayasan pengembangan Teknologi Elektro.

[8] Setiawan, D. (2011). *Mengenal Teknologi VoIP.* Retrieved November 23, 2011, from http://deris.unsri.ac.id/materi/komdat/voip.pdf.

[9] Sopandi, D. (2008). *Instalasi dan Konfigurasi Jaringan Komputer.* Bandung: Informatika.

[10] Sularso, A. d. (2009). *Network Security.* Bandung: Telkom Politeknik.

[11] Wendi, A., & Ramadhana, A. S. (2005). *Membangun VPN Linux secara cepat.* Yogyakarta: Andi.

[12] Ziswandi, M. (2010). *Implementasi Analisis Perbandingan Performansi Jaringan pada VPN Berbasis IPSec dan SSL.* Bandung: Politeknik TELKOM.