Analisa Quality Of Service Dan Implementasi Voice Over Internet Protocol Dengan Menggunakan IPSEC VPN

Ingrid Melyana[1], Tutuk Indriyani[2]
[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya
Email: kagamineingrid@gmail.com

Abstract *At present technology, specifically in telecommunication sector, develops very rapidly, and mainly adopts Internet Protocol (IP) to support the communication network. In IP networks it involves voice communication commonly called Voice over Internet Protocol (VoIP). It the development of telephone communication using IP networks as paths of data transfer. As it is an open source, its network security becomes a crucial issues in VoIP. One of the ways to cope with the security problems is to adopt Intenet Protocol Security (IPSec) in VoIP networks. The communication trials used two different bandwidths – 375 kbps and minimum bandwidth standard – codec G.711 u. The result of the analysis showed that the trial using minimum bandwidth standard – codec G.711 u was not suitable to be applied in VoIP IPSec network, as in average it had package loss by 58.75%. Accordingly, the VoIP IPSec networks with 375 kbps bandwidth were more superior. In average, with delay rate (3,4956 ms), jitter (6,8894 ms) and package loss (0,00%). In conclusion, VoIP IPSec networks requires large bsndwidth, i.e. : minimally 375 kbps in its operation.*

Keywords: Communication, network security, Voice over Internet Protocol (VoIP), Quality of Service, Internet Protocol Security (IPSEC)

Abstrak Pada masa sekarang ini teknologi sangat berkembang pesat, terutama di bidang telekomunikasi. Dan saat ini banyak sekali yang menggunakan jaringan *Internet Protocol* (IP) sebagai jaringan komunikasi. Pada jaringan IP terdapat komunikasi suara yang biasa disebut dengan *Voice Over Internet Protocol* (VoIP) yang merupakan pengembangan dari komunikasi telepon yang menggunakan jaringan IP sebagai jalur transfer datanya. Karena sifatnya yang *opensource*, keamanan jaringan merupakan salah satu permasalahan serius yang terdapat pada VoIP. Salah satu cara untuk mengatasi masalah keamanan tersebut dengan menambahkan metode keamanan IPSec (*Internet Protocol Security*) pada jaringan VoIP. Uji coba komunikasi yang dilakukan menggunakan dua *bandwidth* yang berbeda, menggunakan *bandwidth* 375 kbps dan dengan menggunakan *bandwidth* standar minimum codec G.711u. Dari hasil analisa yang dilakukan, uji coba dengan *bandwidth* standar minimum codec G.711u tidak cocok digunakan pada jaringan VoIP IPSec, karena memiliki kekurangan pada nilai rata-rata *packet loss* sebesar 58,75%. Oleh karena itu jaringan VoIP IPSec lebih unggul bila menggunakan *bandwidth* 375 kbps, dengan keunggulan pada nilai rata-rata *delay* sebesar 3,4956 ms, *jitter* sebesar 6,8894 ms, dan *packet loss* sebesar 0,00%. Sehingga dapat disimpulkan bahwa jaringan VoIP IPSec membutuhkan bandwidth yang besar yaitu minimum 375 kbps dalam penggunaannya.

Kata Kunci : Komunikasi, Keamanan Jaringan, Voice over Internet Protocol (VoIP), Quality of Service, Internet Protocol Security (IPSec)

1. Pendahuluan

a. Latar Belakang

Pada masa sekarang ini teknologi sangat berkembang pesat, terutama di bidang telekomunikasi. Telekomunikasi saat ini perkembangannya lebih mengarah pada jaringan yang berbasis *Internet Protocol* (IP). Komunikasi pada jaringan IP lebih dikenal dengan nama *Voice over Internet Protocol* (VoIP) adalah pengembangan dari komunikasi via PTSN (*Public Switch Telephone Network*) yang menggunakan IP sebagai jalur transfer data. Sistem Jaringan VoIP diciptakan karena sistem jaringan PSTN hanya dapat dikembangkan oleh provider tertentu karena bersifat tertutup. Berbeda dengan jaringan PSTN, VoIP lebih bersifat *opensource* sehingga dapat dikembangkan oleh banyak kalangan. Selain memberikan kemudahaan, VoIP juga memiliki beberapa permasalahan, salah satunya permasalahan tersebut adalah keamanan jaringan.

Karena sifatnya yang *opensource*, VoIP memiliki celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Keamanan jaringan merupakan salah satu permasalahan serius yang terdapat pada VoIP. Sehingga menimbulkan kekhawatiran pada pengguna layanan VoIP. Salah satu cara mengatasi masalah keamanan pada VoIP tersebut adalah dengan menambahkan metode keamanan *Virtual Private Network* (VPN).

VPN (*Virtual Private Network*) merupakan teknologi yang memungkinkan terbentuknya sebuah jaringan data *private* pada jaringan publik dengan menerapkan autentikasi dan enkripsi sehingga akses terhadap jaringan tersebut hanya dapat dilakukan oleh pihak- pihak tertentu. Pada VPN terdapat banyak protokol untuk mendukung keamanan data. Salah satu protokol yang dapat digunakan untuk pengembangan VPN adalah *Internet Protocol Security* (IPSec). IPSec adalah sebuah protokol yang menyediakan transmisi data terenkripsi yang aman pada network layer dalam jaringan

Namun saat ini, paper acuan yang digunakan penulis mencoba menerapkannya menggunakan simulasi. Maka dari itu dalam proyek akhir ini, penulis akan mencoba mengimplementasikan secara *real* untuk mendapatkan hasil yang lebih akurat, dengan membahas analisa *Quality of Service* dan implementasi *Voice over Internet Protocol* dengan menggunakan IPSec VPN.

Dari latar belakang yang telah dijelaskan maka muncul beberapa hal yang perlu diperhatikan, yang pertama bagaimana mengimplementasikan dan merancang VoIP dengan menggunakan metode keamanan IPSec VPN? Yang kedua, bagaimana cara menganalisa kinerja QoS pada VoIP yang telah dirancang dengan menggunakan metode keamanan IPSec VPN?

Berdasarkan penjelasan dari latar belakang diatas maka tujuan dari penelitian ini adalah dapat mengimplementasikan dan merancang VoIP dengan menggunakan metode keamanan IPSec VPN. Kemudian dapat menganalisa kinerja QoS pada VoIP yang telah dirancang dengan menggunakan metode keamanan IPSec VPN.

2. Landasan Teori

Voice over Internet Protocol (VoIP)

Voice Over Internet Protocol (VoIP) adalah layanan *telephone* yang dapat berupa layanan suara, fax, termasuk layanan voice messaging yang ditransmisikan dalam bentuk paket melalui jaringan berbasis *Internet Protocol* (Anton,2008).

Teknologi VoIP pada dasarnya bekerja dengan mengkonversi sinyal- sinyal analog ke format digital dan kemudian dikompres atau ditranslasikan ke dalam paket- paket IP yang kemudian ditransmisikan melalui jaringan internet atau intranet. Pada Gambar 1. memperlihatkan konsep cara kerja VoIP (Anwar,2015).

Gambar 1. Cara kerja VoIP

Beberapa keuntungan penggunaan VoIP baik dari sisi pengguna, maupun penyedia jasa *internet telephone* adalah :

1. ***Cost reduction***
   Dengan adanya fitur *silence suppression* dan *voice activity detection* (VAD), *bandwidth* jaringan yang ada dapat sekaligus dipakai untuk transmisi data dan suara. selain itu, karena informasi dikirimkan dalam bentuk paket. Satu kanal dapat dipakai bersama-sama, sehingga biaya percakapan untuk interlokal dan internasional dapt direduksi. Reduksi biaya waktu percakapan mencapai 50% - 60%.
2. ***Simplification***
   Integrasi jaringan voice dan data memudahkan standarisasi dan minimalisasi perangkat yang digunakan.
3. ***Consolidation***
   Kemampuan penanganan gangguan, dan konsolidasi serta kombinasi operasional yang lebih efisien.
4. ***Advanced application***
   Keuntungan jangka panjang dari VoIP meliputi *support* untuk *multimedia* dan aplikasi *multiservice*.

***Quality of Service* (QoS)**

Quality of Service didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan kerakteristik dan sifat dari suatu layanan. QoS mengacu pada kemampuan jarigan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Beberapa parameter QoS yaitu *delay, jitter, throuthput, dan packet loss*.

Delay dapat didefinisikan sebagai waktu yang dibutuhkan untuk mengirimkan data dari sumber (pengirim) ke tujuan (penerima). *Delay* dapat dihitung dengan menggunakan rumus :

$$Rata - Rata\ delay = \frac{Total\ Delay}{Total\ paket\ yang\ diterima} \quad (1)$$

Tabel 1. Standar *Delay* Berdasarkan ITU-T G.114

Kategori Delay	Besar *Delay*
Sangat Bagus	<150 ms
Bagus	150 ms s/d 300 ms
Jelek	300 ms s/d 450 ms
Sangat Jelek	> 450 ms

Jitter disebabkan oleh bervariasinya waktu penerimaan pengiriman paket-paket data dari pengirim ke penerima. *Jitter* dihitung menggunakan rumus :

$$Jitter = \frac{total\ variasi\ delay}{total\ paket\ yang\ diterima - 1} \quad (2)$$

Total Variasi *delay* diperoleh dari penjumlahan :

(*delay* 2 – *delay* 1) + (*delay* 3 – *delay* 2) +… + (*delay* n – *delay* (n-1)) (3)

Berdasarkan Standar ITU-T telah ditetapkan standar *Jitter* yang dapat diterima/ditoleransi.

Tabel 2. Standar *Jitter*

Kategori *Jitter*	Besar *Jitter*
Baik	0 – 20 ms
Cukup	20 ms – 50 ms
Buruk	> 50 ms

Pada jaringan berbasis IP, semua *frame* suara diperlakukan sama seperti *frame* data. Pada saat *peak load* dan *congestion*, *frame* suara akan dibuang sama dengan *frame* data. *Frame* suara sensitif terhadap waktu sehingga bila dilakukan retransmisi akan mengubah arti pembicaraan. *Packet Loss* dapat dihitung menggunakan rumus :

$$Packet\ Loss = \frac{P.data\ yang\ dikirim - P.data\ yang\ diterima}{P.data\ yang\ dikirim}\ x\ 100\% \quad (4)$$

Tabel 3. Standar *Packet Loss*

Kategori *Packet Loss*	*Packet Loss*
Baik	0 - 1%
Cukup	1% - 5%
Kurang	5% - 10%
Buruk	> 10%

Throughput, adalah jumlah total kedatangan paket IP sukses yang diamati di tempat pengukuran pada *destination* selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut (sama dengan, jumlah pengiriman paket IP sukses per *service-second*).

Untuk menghitung *Througput* menggunakan rumus :

$$Throughput = \frac{paket\ data\ yang\ diterima}{lama\ pengamatan} \quad (5)$$

Metode pengukuran subyektif yang umum dipergunakan dalam pengukuran kualitas *speech coder* adalah ACR (*Absolute Category Rating*) yang akan menghasilkan nilai MOS (*Mean Opinion Score*). Tes subyektif ACR meminta pengamat untuk menentukan kualitas suatu *speech coder* tanpa membandingkannya dengan sebuah referensi. Bila pengukuran dengan objektif maka pengukuran MOS menggunakan parameter QoS, yaitu *delay, jitter, packet loss* yang didapat pada saat pengukuran. Skala rating umumnya mempergunakan penilaian yaitu berturut-turut : *Exellent, Good, Fair, Poor,* dan *Bad* dengan nilai MOS berturut-turut : 5, 4, 3, 2, dan 1.

Bandwidth merupakan kecepatan maksimum yang dapat digunakan untuk melakukan transmisi data antar jaringan IP atau internet. Untuk menghitung *bandwidth* menggunakan rumus:

$$Bandwidth = total\ packet\ size * PPS \quad (6)$$

Total *Packet Size* diperoleh dengan perhitungan :

(L2 header: MP or FRF.12 or Ethernet) + (IP/UDP/RTP header) + (voice payload size) (7)

PPS diperoleh dengan perhitungan :

(codec bit rate) / (voice payload size) (8)

Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam kantor atau network itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik (Afrianto,2014).

Jenis Implementasi VPN

1. ***Remote Access* VPN**

   Remote access yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN). Biasanya akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan dan *software client* untuk pegawai perusahaan.

2. ***Site-to-Site* VPN**

   Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara dua kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya.

***Internet Protocol Security* (IPSec)**

IPsec merupakan suatu set ektensi protokol dari *Internet Protocol* (IP) yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). Istilah dari IPsec mengacu pada suatu set dari mekanisme yang didesain untuk mengamankan trafik pada level IP atau pada network layer (Kurniawan,2011).

Teknologi dari IPsec ini didasari oleh teknologi modern dari kriptografi, dimana layanan keamanan yang disediakan antara lain yaitu:

1. ***Confidentiality***

   Untuk mejamin kerahasiaan dimana sulit bagi pihak yang tidak berwenang untuk dapat melihat atau mengerti kecuali oleh penerima yang sah bahwa data telah dikirimkan.

2. ***Integrity***

   Untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

3. ***Authenticity***

   Untuk menjamin bahwa data yang dikirimkan memang berasal dari pengirim yang benar.

4. ***Anti Reply***

   Untuk menjamin bahwa transaksi hanya dilakukan sekali, kecuali yang berwenang telah mengijinkan untuk mengulang transaksi.

Protokol IPSec

1. ***Authentication Header* (AH)**

   Menyediakan layanan *authentication, integrity, replay protection* pengamanan pada *header* IP, namun tidak menyediakan layanan *confidentiality*.

2. Encapsulating Security Payload(ESP)

Menyediakan layanan *authentication, integrity, replays protection* dan *confidentiality* terhadap data (ESP melakukan pengamanan data terhadap segala sesuatu dalam paket data setelah *header*).

Arsitektur IPSec

Perkembangan arsitektur IPSec mengacu pada pokok persoalan yang terdapat pada RFC. Terdapat tujuh bagian utama yang dapat digunakan untuk mendefinisikan keseluruhan arsitektur dari IPSec.

1. *Architecture*

Mencakup konsep secara umum, definisi, kebutuhan keamanan, dan mekanisme yang mendefinisikan teknologi dari IPSec.

2. *Encapsulating Security Payload* (ESP)

Menyediakan layanan kerahasiaan data dengan enkripsi, enkapsulasi, dan secara opsional yaitu autentikasi.

3. *Authentication Header* (AH)

Menyediakan mekanisme untuk autentikasi sumber data dan layanan *connection less data integrity* untuk paket IP.

4. *Encryption Algorithm*

Menyediakan bermacam-macam algoritma enkripsi yang digunakan oleh ESP.

5. *Authentication Algorithm*

Menyediakan algoritma autentikasi yang digunakan oleh AH dan secara opsional digunakan pula oleh ESP, seperti HMAC-MD5-96, HMAC-SHA-1-96

6. *Domain of Interpretation* (DOI)

Mendefinisikan format payload, pertukaran tipe dan konvensi untuk penamaan terhadap informasi keamanan yang relevan. DOI juga mengandung nilai-nilai yang dibutuhkan untuk menghubungkan bagian satu dengan yang lainnya.

7. *Key Management*

Mengandung dokumen yang menggambarkan bermacam-macam skema dari manajemen pertukaran kunci.

IPSec *Modes*

Terdapat dua mode dalam implementasi dari IPSec, yaitu sebagai berikut:

1. Mode pertama yang digunakan yaitu *transport mode*. Secara umum mode ini digunakan untuk komunikasi end-to-end antar dua host. Contohnya komunikasi *client-server*.
2. Mode implementasi kedua dari IPsec yaitu *tunnel mode. Tunnel mode* menyediakan proteksi untuk keseluruhan paket IP. Dimana gateway mengenkapsulasi keseluruhan paket, termasuk original header dari IP, kemudian menambahkan header IP baru pada paket data, lalu mengirimkannya ke jaringan publik menuju gateway yang kedua, dimana informasi akan di dekripsi dan bentuk asli informasi akan sampai ke penerima.

Cara Kerja IPSec

IPSec menggunakan dua protocol untuk menyediakan sekuritas trafik, yaitu Authentication Header (AH) dan Encapsulating Security Payload (ESP) Kedua-duanya, AH dan ESP, adalah kendaraan untuk kontrol akses, berdasarkan distribusi kunci kriptografi dan manajemen laju trafik relatif terhadap protocol keamanan tersebut. Masing-masing protokol mendukung dua mod penggunaan yaitu mode transport dan mode tunnel. Dalam mode transport, protocol menyediakan proteksi terutama untuk protokol layer yang lebih tinggi Sedangkan dalam mode tunnel, protokol diaplikasikan pada paket IP yang di tunnel (Muthohar,2009).

IPSec mengizinkan pengguna (atau administrator sistem) untuk mengontrol granularitas di mana servis keamanan ditawarkan. Sebagai contoh, seseorang dapat menciptakan sebuah tunnel terenkripsi tunggal untuk membawa semua trafik diantara dua gateway keamanan atau tunnel terenkripsi yang terpisah dapat dibuat untuk setiap koneksi TCP di antara pasangan host yang saling berkomunikasi melalui gateway tersebut. Manajemen IPSec harus menggabungkan fasilitas untuk menspesifikasikan:

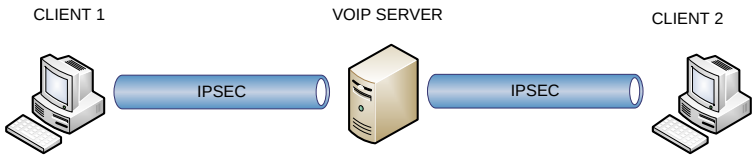
1. Servis sekuritas mana yang akan digunakan dan dengan kombinasi seperti apa.
2. Granularitas di mana sebuah proteksi sekuritas seharusnya diterapkan.
3. Algoritma yang digunakan untuk menghasilkan sekuritas berdasar kriptografi

Karena servis sekuritas tersebut digunakan untuk berbagi nilai rahasia (kunci kriptografi), IPSec bergantung pada sejumlah mekanisme terpisah untuk meletakkan kunci tersebut pada tempatnya. Kunci tersebut digunakan untuk autentikasi/intregritas dan servis enkripsi.

3. Perancangan Sistem

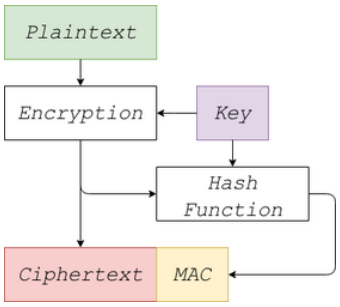
Desain Sistem

Dengan perancangan Analisis *Quality of Service* dan Implementasi *Voice Over Internet Protocol* dengan menggunakan IPSec VPN, penulis ingin menganalisa beberapa parameter meliputi *Delay, Throughput, Jitter, Packet Loss,* dan *Bandwidth* . Dari analisa *Quality of Service* pada VoIP ini akan diketahui bagaimana *Quality of Service* pada VoIP yang telah menggunakan metode keamanan dan bagaimana cara untuk mengoptimalkan *Quality of Service* pada VoIP yang telah menggunakan metode keamanan tersebut. Dibawah ini merupakan gambaran dari desain sistem dalam penelitian ini.



Gambar 2. Desain Sistem Jaringan VoIP

Pada gambar 2. dijelaskan antara client satu dengan client lainnya saling berkomunikasi melalui voip server. Dimana akan diberi metode keamanan dengan IPSec VPN.



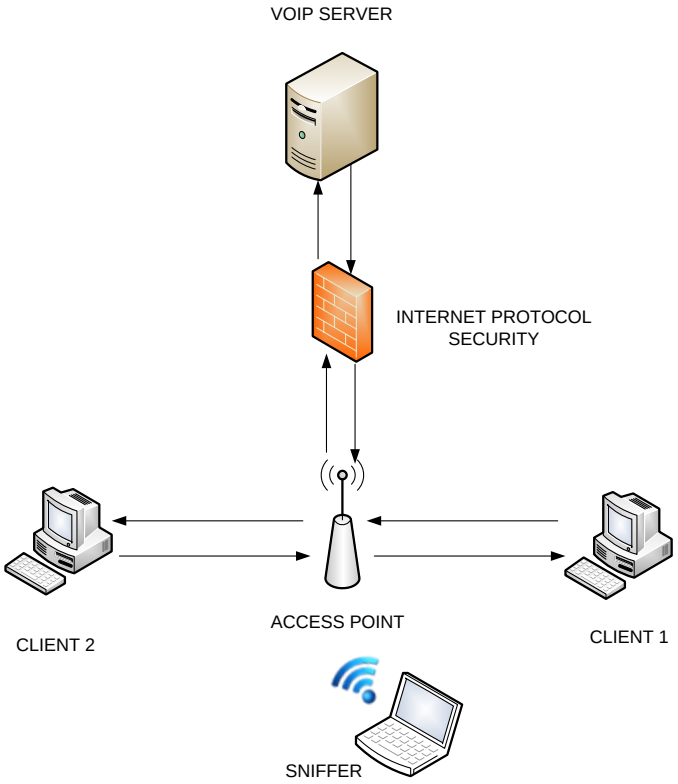
Gambar 3. Cara Kerja IPSec

Pada gambar 3. merupakan sebuah gambar yang menjelaskan cara kerja IPSec VPN. Yang pertama, pesan akan dienkripsi menjadi chipertext dan di autentikasi. Kemudian akan menghasilkan MAC (*Message Authentication Code*) yang akan ditambahkan pada chipertext. Hal ini memberikan

chipertext integritas. Keuntungannya adalah bila MAC tidak sesuai selama proses verifikasi, chipertext tidak akan didekripsikan.

Desain Arsitektur Jaringan

Rancangan arsitektur jaringan dalam penelitian ini menggunakan *Local Area Network* (LAN) dan *Wireless Local Area Network* (W*LAN*), dimana server VOIP dan dua *user* terhubung di dalam satu jaringan menggunakan *Access Point*. Berikut adalah gambar arsitektur jaringan dari penelitian ini :

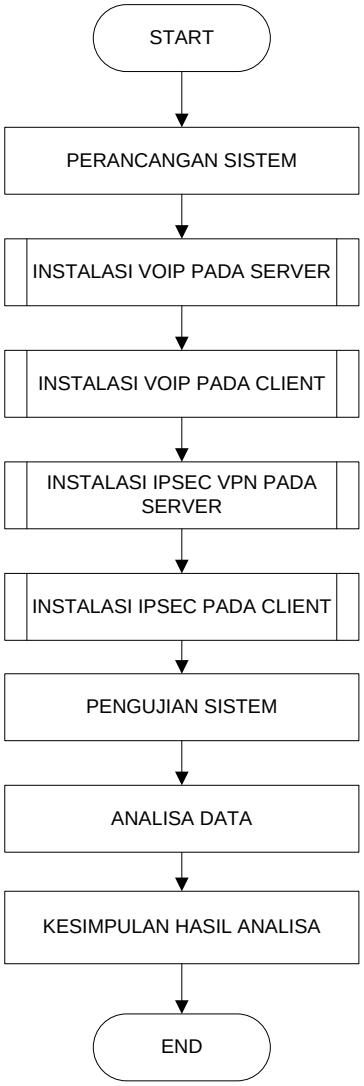


Gambar 4. Arsitektur Jaringan

Desain Sistem

Jaringan VoIP pada penelitian ini menggunakan sebuah VoIP *Server* dengan keamanan berbasis *Internet Protocol Security* yang berfungsi untuk meningkatkan keamanan berkomunikasi di jaringan VoIP. Dengan menggunakan *Internet Protocol Security* semua data yang melewati jaringan VoIP tersebut akan dienkripsi sehingga meningkatkan keamanan terhadap pihak yang tidak berkepentingan.

Berikut merupakan gambar diagram alur untuk mengerjakan penelitian ini.



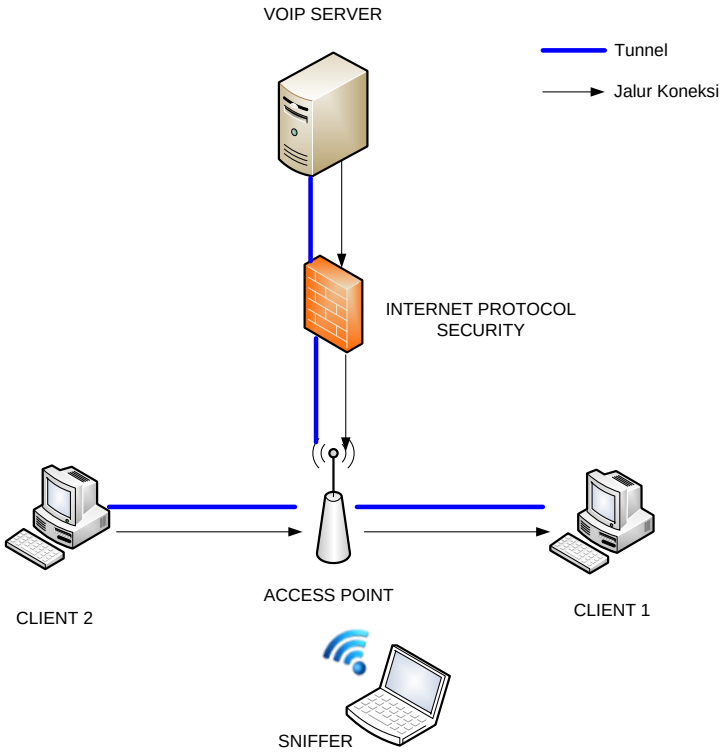
Gambar 5. Alur Perancangan dan Implementasi

Desain Pengujian Sistem

Fungsi utama VoIP adalah untuk memudahkan berkomunikasi melalui internet. VoIP akan mengubah suara yang diterima menjadi sinyal digital kemudian sinyal digital tersebut akan dikirimkan ke tujuan melalui internet.

Pada saat client 1 akan berkomunikasi dengan client 2, atau client 1 ingin berkomunikasi dengan server. Ada kemungkinan komunikasi akan disadap oleh pihak yang tidak berkepentingan, misalnya sniffer. Penyadapan dilakukan dengan menyadap paket data yang melewati jaringan tersebut.

Topologi dapat dilihat seperti gambar 6.



Gambar 6. Desain Pengujian Sistem

Pada gambar 6. menjelaskan tahapan komunikasi antara *client* 1 VoIP dan *client* 2 VoIP ketika komunikasi mulai dilakukan hingga komunikasi antara *client* 1 dan *client* 2 VoIP berakhir. IPSec akan membuat Tunnel atau jalur rahasia, dimana paket data yang melewati tunnel tersebut dienkripsi sehingga tidak akan diketahui oleh pihak-pihak yang tidak berkepentingan.

4. Implementasi Sistem

Pengujian Sistem

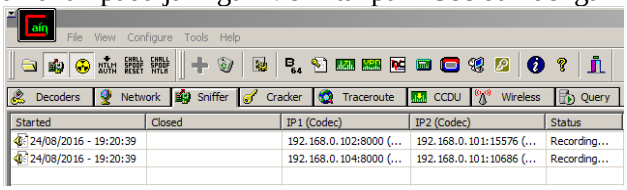
Pada tahap pengujian sistem, penulis melakukan uji coba komunikasi antara *client* 1 dengan *client* 2 menggunakan jaringan VoIP. Berikut merupakan tahap-tahap pengujian yang dilakukan :

1. Memastikan dan melakukan pengecekan pada tiap client apakah *softphone* client telah terdaftar pada server VoIP yaitu ekstensi 111 dan 222.
2. Sebelum melakukan panggilan, jalankan program capture.py untuk dapat meng-capture komunikasi yang akan berlangsung.
3. Setelah dipastikan terdaftar maka yang selanjutnya dilakukan adalah melakukan panggilan antar akun.
4. Pengujian dilakukan dengan melakukan panggilan selama 1 menit. Lalu putuskan komunikasi dan hentikan program capture yang berjalan dengan menekan Ctrl+C. Kemudian jalankan program analisa.py agar komunikasi yang telah terjadi dapat dianalisa.

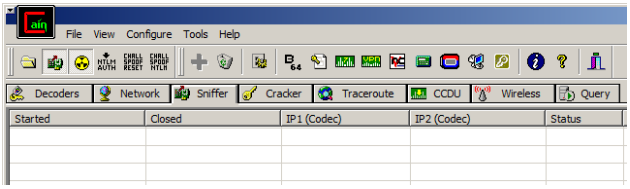
Pengujian Keamanan

Pengujian kemanan pada penelitian ini dilakukan dengan Teknik *Sniffing* . *Sniffing* dilakukan tanpa merubah data atau paket apapun pada jaringan, *Sniffer* akan melakukan penyadapan terhadap komunikasi *Client-Server* yang sedang berjalan pada jaringan local, dimana pada ada saat *Client*1 sedang melakukan komunikasi ke *Client* 2 yang melewati *Server* terlebih dahulu.

Proses sniffing dilakukan dengan menggunakan aplikasi Cain & Abel. Berikut adalah gambar hasil pengujian keamanan pada jaringan VoIP tanpa IPSec dan dengan IPSec:



Gambar 7. *Sniffing* VoIP non IPSec



Gambar 8. *Sniffing* VoIP IPSec

Pada gambar 7. , *sniffer* dapat menyadap komunikasi antara *client*1 dan *client*2 pada jaringan VoIP tanpa keamanan. Sedangkan pada gambar 8., untuk jaringan VoIP yang telah diberi kemananan IPSec, komunikasi antara *client* 1 dan *client* 2 tidak dapat disadap oleh *sniffer*.

Analisa Sistem

Analisa dilakukan dengan menggunakan 2 *bandwidth* dan juga telah dilakukan analisa QoS yang meliputi perbandingan *Delay*, *Jitter*, *Throughput*, dan *Packet Loss* pada jaringan VoIP tanpa IPSec terhadap jaringan VoIP IPSec. Berikut merupakan beberapa tabel hasil perbandingan yang telah diperoleh :

Tabel 4. Analisa Perbandingan kualitas *Delay*

Percobaan Ke-	***Delay* (ms)**			
	Non IPSec		**IPSec**	
	***Bandwidth* 375 kbps**	***Bandwidth* Standar**	***Bandwidth* 375 kbps**	***Bandwidth* Standar**
1	5.007	6.702	3.508	7.492
2	5.006	6.744	3.499	7.728
3	5.004	6.724	3.508	7.419
4	5.004	6.730	3.479	7.387
5	5.005	6.684	3.480	7.784
6	5.003	6.663	3.496	7.394
7	5.003	6.668	3.509	7.467
8	5.006	6.683	3.489	7.356
9	5.004	6.668	3.499	7.684
10	5.004	6.676	3.489	7.390
Total	50.046	66.942	34.956	75.101
Rata-Rata	5.0046	6.6942	3.4956	7.5101

Dari hasil analisa *delay* pada tabel 4. terlihat bahwa uji coba dengan *bandwidth* 375 kbps pada jaringan VoIP non IPSec memiliki rata-rata nilai 5.0046 ms dan VoIP IPSec memiliki rata-rata nilai 3.4956 ms. Kemudian untuk uji coba dengan *bandwidth* standar minimum codec G.711u pada jaringan VoIP non IPSec memiliki *delay* lebih kecil daripada jaringan VoIP IPSec, dimana VoIP non IPSec memiliki rata-rata nilai 6.6942 ms dan VoIP IPSec memiliki rata-rata nilai 7.5101 ms.

Tabel 5. Analisa Perbandingan kualitas *Jitter*

***Jitter* (ms)**				
Percobaan Ke-	**Non IPSec**		**IPSec**	
	***Bandwidth* 375 kbps**	***Bandwidth* Standar**	***Bandwidth* 375 kbps**	***Bandwidth* Standar**
1	9.8927	9.9458	6.9176	11.6240
2	9.8881	10.7563	6.9208	12.1024
3	9.8851	9.5621	6.9201	9.1589
4	9.8954	9.7321	6.8803	9.6705
5	9.8823	11.1791	6.8495	9.6237
6	9.8965	10.3605	6.8892	12.7557
7	9.9005	9.9488	6.8499	13.0170
8	9.8954	8.9458	6.8890	12.1264
9	9.8950	9.6471	6.8986	9.1033
10	9.8959	10.9168	6.8790	10.3612
Total	98.9269	100.9944	68.894	109.5431
Rata-Rata	9.89269	10.09944	6.8894	10.95431

Dari hasil analisa *jitter* pada tabel 5. terlihat bahwa uji coba dengan *bandwidth* 375 kbps pada jaringan VoIP non IPSec memiliki rata-rata nilai 9.89269 ms dan VoIP IPSec memiliki rata-rata nilai 6.8894 ms. Kemudian untuk uji coba dengan *bandwidth* standar minimum codec G.711u pada jaringan VoIP non IPSec memiliki *jitter* lebih besar daripada jaringan VoIP IPSec, dimana VoIP non IPSec memiliki rata-rata nilai 10.09944 ms dan VoIP IPSec memiliki rata-rata nilai 10.95431 ms.

Tabel 6. Analisa Perbandingan kualitas *Throughput*

***Throughput* (kbps)**				
Percobaan Ke-	**Non IPSec**		**IPSec**	
	***Bandwidth* 375 kbps**	***Bandwidth* Standar**	***Bandwidth* 375 kbps**	***Bandwidth* Standar**
1	341.945	252.502	587.589	281.067
2	342.015	253.885	588.284	271.144
3	342.124	254.668	586.795	282.104
4	342.172	254.415	591.702	283.505
5	341.071	256.198	593.338	269.538
6	342.178	256.952	588.825	283.740
7	342.201	256.023	591.593	281.063
8	342.024	256.211	589.909	286.485
9	342.154	256.779	588.296	272.824
10	342.098	256.479	590.678	283.435
Total	3419.982	2554.112	5897.009	2794.905
Rata-Rata	341.9982	255.4112	589.7009	279.4905

Dari hasil analisa *throughput* pada tabel 6. terlihat bahwa uji coba dengan *bandwidth* 375 kbps pada jaringan VoIP non IPSec memiliki rata-rata nilai 341.9982 kbps dan VoIP IPSec memiliki rata-rata nilai 589.7009 kbps. Kemudian untuk uji coba dengan *bandwidth* standar

minimum codec G.711u pada jaringan VoIP non IPSec memiliki throughput lebih kecil daripada jaringan VoIP IPSec, dimana VoIP non IPSec memiliki rata-rata nilai 255.4112 kbps dan VoIP IPSec memiliki rata-rata nilai 279.4905 kbps.

Tabel 7. Analisa Perbandingan kualitas *Packet Loss*

Percobaan Ke-	Packet Loss (%)			
	Non IPSec		IPSec	
	***Bandwidth* 375 kbps**	***Bandwidth* Standar**	***Bandwidth* 375 kbps**	***Bandwidth* Standar**
1	0.00	0.86	0.00	58.8
2	0.00	0.90	0.00	58.3
3	0.00	0.90	0.00	58.2
4	0.00	1.14	0.00	58.5
5	0.00	1.15	0.00	58.6
6	0.00	0.84	0.00	59.4
7	0.00	0.82	0.00	59.5
8	0.00	0.71	0.00	59.1
9	0.00	0.02	0.00	58.5
10	0.00	0.83	0.00	58.6
Total	0.00	8.17	0.00	587.5
Rata-Rata	0.00	0.817	0.00	58.75

Dari hasil analisa *packet loss* pada tabel 7. terlihat bahwa uji coba dengan *bandwidth* 375 kbps pada jaringan VoIP non IPSec memiliki nilai rata-rata packet loss yang sama dengan jaringan VoIP IPSec, yaitu sebesar 0%. Dan pada uji coba dengan *bandwidth* standar minimum codec G.711u pada jaringan VoIP non IPSec memiliki nilai rata-rata *packet loss* lebih kecil daripada jaringan VoIP IPSec, dimana VoIP non IPSec memiliki rata-rata nilai 0.817% dan VoIP IPSec memiliki rata-rata nilai 58.75%.

4. Penutup

Kesimpulan

Dari analisis *Quality of Service* dan implementasi *Voice over Internet Protocol* dengan menggunakan IPSec VPN ini dapat ditarik kesimpulan bahwa :

1. Nilai rata-rata dari parameter *Delay* untuk *bandwidth* 375 kbps memiliki nilai lebih kecil daripada *bandwidth* standar minimum codec G.711u karena semakin besar *bandwidth* yang digunakan maka nilai *delay* akan semakin kecil dan jumlah paket yang diterima semakin banyak. Untuk *bandwidth* 375 kbps pada VoIP non IPSec memiliki nilai rata-rata sebesar 5.0046 ms dan pada VoIP IPSec sebesar 3.4956 ms. Sedangkan untuk *bandwidth* standar pada VoIP non IPSec sebesar 6.6942 ms dan pada VoIP IPSec sebesar 7.5101 ms.

2. Nilai rata-rata dari parameter Jitter untuk bandwidth 375 kbps memiliki nilai lebih kecil daripada bandwidth standar minimum codec G.711u karena semakin besar bandwidth yang digunakan maka delay akan semakin kecil dan jitter pun juga akan lebih kecil karena jitter adalah variasi waktu delay. Untuk bandwidth 375 kbps pada VoIP non IPSec memiliki nilai rata-rata sebesar 9.89269 ms dan pada VoIP IPSec sebesar 6.8894 ms.. Sedangkan untuk bandwidth standar minimum codec G.711u pada VoIP non IPSec sebesar 10.09944 ms dan pada VoIP IPSec sebesar 10.95431
3. Nilai rata-rata dari parameter Throughput untuk bandwidth 375 kbps memiliki nilai lebih besar daripada bandwidth standar minimum codec G.711u. Semakin besar bandwidth yang digunakan maka semakin besar pula nilai throughput karena throughput adalah bandwidth yang sebenarnya. Untuk bandwidth 375 kbps pada VoIP non IPSec memiliki nilai rata-rata

sebesar 341.9982 kbps dan pada VoIP IPSec sebesar 589.7009 kbps. Sedangkan untuk bandwidth standar minimum codec G.711u pada VoIP non IPSec sebesar 255.4112 kbps dan pada VoIP IPSec sebesar 279.4905 kbps.

4. Nilai rata-rata dari parameter Packet Loss untuk bandwidth 375 kbps pada VoIP non IPSec memiliki nilai sama dengan VoIP IPSec yaitu sebesar 0%. Sedangkan untuk bandwidth standar minimum codec G.711u pada VoIP non IPSec sebesar 0.817% dan pada VoIP IPSec sebesar 58.75%. Nilai packet loss sangat besar dikarenakan bandwidth yang digunakan kurang dari bandwidth minimum yang dibutuhkan.
5. Secara garis besar, pada jaringan VoIP IPSec dengan bandwidth 375 kbps lebih cocok digunakan daripada menggunakan bandwidth standar minimum codec G.711u. Bila menggunakan bandwidth standar minimum codec G.711u, untuk VoIP non IPSec masih cocok untuk digunakan. Namun untuk VoIP IPSec, sangat tidak cocok untuk digunakan karena pada VoIP IPSec memiliki nilai rata-rata packet loss sebesar 58.75% . Dan itu berarti jumlah paket yang diterima kurang dari setengah dari yang dikirimkan.

Saran

Dari hasil analisa yang telah dibuat, diketahui bahwa VoIP dengan menggunakan IPSec membutuhkan *bandwidth* yang besar dalam penerapannya sehingga tidak memungkinkan untuk penerapan dengan user berskala besar . Untuk pengembangan lebih lanjut, alangkah baiknya bila *bandwidth* yang dibutuhkan VoIP IPSec dapat di minimalisir, sehingga VoIP IPSec dapat diterapkan setidaknya pada *small office.*

DAFTAR PUSTAKA

Afrianto, Irawan dan Setiawan, Eko Budi. (2014). *Kajian Virtual Private Network(VPN) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom).* Bandung : Universitas Komputer Indonesia.

Anton dan Anggraini, Rina. (2008). *Sistem Teknologi Voice over IP (VoIP)*. Padang : Politeknik Negeri Padang.

Anwar, Hawira dan Sani, Arman. (2015). *Analisis Kualitas Layanan Sistem Telepon VoIP Memanfaatkan Jaringan Wifi USU*. Sumatera Utara : Universitas Sumatera Utara.

Babu, Masqueen. (2012). *Performance Analysis of IPSec VPN over VoIP Networks Using OPNET*. Jalandhar : Dr. B. R. Ambedkar National Institute of Technology.

Kurniawan, Helmi dan Rahmad, Iwan Fitrianto. (2011). *Analisa Interkoneksi Internet Protocol Security Pada Jaringan Komputer Berbasis Network Address Translation.* Medan : STMIK Potensi Utama.

Muthohar, Muhammad Fiqri. (2009). *Studi Penerapan Beberapa Algoritma Kriptografi pada IPSec.* Bandung : Institut Teknologi Bandung.