RANCANG BANGUN KEAMANAN TRANSFER DATA VOIP MENGGUNAKAN VPN PADA TRIXBOX DI UNIVERSITAS SATYA NEGARA INDONESIA

Faizal Zuli[1], Meri Kristina Br Sinuraya[2]
Fakulas Teknik, Universitas Satya Negara Indonesia
faizal.zuli@yahoo.com, merysinuraya158@gmail.com

ABSTRAK

VoIP (Voice Over Internet Protocol) merupakan suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan media protokol IP. *VoIP* bekerja dengan mengubah sinyal analog menjadi sinyal *digital*. Penggunaan jaringan IP menghemat biaya karena tidak perlu membangun infrastruktur baru untuk komunikasi suara dan penggunaan *bandwidth* lebih kecil dibanding telepon konvensional.
Kata Kunci : VOIP, Jaringan Komputer, Nirkabel, Koneksi Data

ABSTRACT

VoIP (Voice Over Internet Protocol) is a system that uses the internet network to transmit voice packet data from one place to another using the IP protocol media. VoIP works by converting analog signals into digital signals. The use of IP networks saves costs because there is no need to build new infrastructure for voice communications and use less bandwidth than conventional telephones.
***Keywords** : VOIP, Computer Network, Wireless, Data Connection*

PENDAHULUAN

Universitas Satya Negara Indonesia (USNI) berdiri sejak 1989 dan di naungi oleh Yayasan Abdi Karya (YADIKA). Sebagai salah satu perguruan tinggi, sistem komunikasi yang di gunakan karyawan, staff dan pegawai di USNI masih menggunakan telepon kabel untuk alat komunikasi di lingkungannya. Dalam penggunaan telepon kabel biaya setiap panggilan masih terbilang mahal, dan tidak seperti penggunaan VoIP. Penggunaan VoIP sangat menguntungkan, namun keamanan pada sistem ini kurang diperhatikan, karena transfer data pada VoIP berbasis IP maka mudah di sadap dan dapat dilakukan perekaman data VoIP. Jika data yang ditangkap ternyata rahasia maka akan sangat merugikan, bahkan bisa disalahgunakan. Hal ini menyebabkan kurangnya kemanan dan privasi pengguna VoIP.

Dari Masalah tersebut penulis tertarik untuk melakuan penelitian dengan merancang dan membangun jaringan VoIP ini dengan menggunakan TrixBox berikut juga pengamanannya dengan menggunakan jaringan VPN.

Rumusan Masalah

Berdasarkan latar belakang yang telah di uraikan diatas, maka penulis merumuskan beberapa pokok masalah yang diteliti :

1.Bagaimana membangun system komunikasi VoIP menggunakan server Trixbox ?
2.Bagaimana mengamankan komunikasi VoIP dengan VPN (Virtual Privat Netwok) ?
3.Bagaimana hasil dari pengujian parameter QoS pada system VoIP yang dibangun ?

Batasan Masalah

Agar lebih mengarah dan tidak menyimpang dari penelitian, maka penelitian ini dibatasi sebagai berikut :

1. System komunikasi VoIP dibangun menggunakan server Trixbox
2. Rancangan Keamanan Transfer Data VoIP ini, hanya menggunakan jalur VPN (Virtual Private Network).
3. Pengujian QoS pada system VoIP yang dibangun

Tujuan Penelitian

Tujuan dilakukannya Penelitian Tugas Akhir ini adalah Melakukan Rancang Bangun Keamanan Transfer Data VoIP Menggunakan VPN Pada Trixbox di Universitas Satya Negara Indonesia.

Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dapat membangun komunikasi system VoIP dengan server Trixbox
2. Mengamankan jalur komunikasi antar client dengan VPN (Virtual Privat Network)
3. Dapat menghemat biaya panggilan komunikasi

Tinjauan Pustaka

Pada penelitian ini diperlukannya tinjauan pustaka sebagai pendukung dalam penelitian ini, beberapa topik yang berkaitan dengan penulisan penelitian ini adalah:

1. Rancang Bangun Keamanan Transfer Data VoIP Over VPN Pada Sistem Opensource Trixbox". VoIP merupakan suatu sistem yang menggunakan jaringan internet untuk mengirimkan paket data suara dari suatu tempat ke tempat yang lain menggunakan protokol IP. VoIP dapat mengurangi biaya panggilan hingga 70%. Namun terdapat beberapa masalah yang dialami ketika menggunakan VoIP, salah satunya transfer data yang lewat pada jaringan dapat disalahgunakan, dan dibajak. Oleh karenanya untuk mengamankan paket yang lewat maka digunakan teknologi VPN (Virtual Privat Network). VPN mempunyai dua teknik pengamanan yaitu IPSec dan Cripto IP Encapculation. Untuk mengatasi penyadapan pada penggunaan VoIP maka dilakukan penambahan VPN server pada Trixbox, serta penambahan VPN client pada sisi client VoIP, sehingga trafik VoIP dilewatkan melalui jaringan VPN. Penggunaaan VPN ini menjadikan sistem VoIP aman karena adanya enkripsi dan autentikasi antara client dan server.

2. (Azhar, Badrul, & Akmaludin, 2018) "Penerapan Voice Over Internet Protokol (VoIP) Untuk Optimalisasi Jaringan Pada Badan Kependudukan dan Keluarga Berenca Nasional". BKKBN merupakan lembaga pemerintah yang bertugas untuk mewujudkan keluarga berencana dan keluarga sejahtera. Dalam melaksanakan tugasnya salah satu hal yang menunjang keberhasilan program ini adalah kelancaran komunikasi. Adapun masalah yang dialami oleh BKKBN adalah kurang optimalnya jaringan komunikasi dari pusat BKKBN dengan wilayah Indonesia bagian timur, yaitu Maluku Utara dan Papua Barat. Hal ini di sebabkan karena wilayah tersebut masih menggunakan telepon konvensional sebagai alat komunikasinya.Untuk melakukan optimalisasi jaringan tersebut maka BKKBN harus menerapkan implementasi jaringan VoIP. Dan untuk keamanannya BKKBN Pusat menggunakan teknologi VPN (Virtual Privat Network). Dengan begitu semua percakapan yang dilakukan BKKBN akan terjamin keamanannya.

VOIP (Voice Over Internet Protocol)
VoIP dikenal juga dengan sebutan IP Telephony didefinisikan sebagai suatu sistem yang menggunakan jaringan internet sebagai media transport informasi/data. Informasi VoIP dibawa melalui media IP, bukan media telephony (Kristalina, 2015).

Sejarah VoIP
Sejarah Perkembangan teknologi VoIP dimulai dari penemuan telepon pada tahun 1876 oleh Alexander Graham Bell. Kemudian dikembangkan lagi teknologi PSTN (Public Switched Telephone Network) yang sudah berkembang sampai sekarang. Beberapa tahun kemudian mulai berkembang teknologi yang baru. Pembuatan Personal Computer (PC) secara massal, system komunikasi telepon selular dan system berdasarkan jaringan internet. Teknologi VoIP diperkenalkan setelah internet mulai berkembang sekitar tahun 1995. Ini dimulai dengan perusahaan seperti Vocaltech dan kemudian pada akhirnya diikuti oleh Microsoft dengan program Netmeeting-nya.

Kualitas Jaringan VoIP

VoIP merupakan salah satu jenis layanan *realtime* yang membutuhkan QoS *(Quality of Service)*. Beberapa faktor yang memengaruhi Qos adalah:

a. *Delay*
Delay merupakan waktu yang dibutuhkan untuk mengirimkan suatu paket data dari sumber ke penerima . Berikut adalah standar delay berdasarkan ITU *(International Communication Union)*

Tabel 1 Kualitas *Delay*

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

Semakin besar *delay* yang dihasilkan maka semakin rendah kualitas VOIP yang di hasilkan. *Delay* dapat di hitung dengan rumus sebagai berikut *:*

$$\text{Rata -rata Delay} = \frac{\text{Total Delay}}{\text{Total Paket Yang Diterima}}$$

b. *Packet Loss*
Packet Loss merupakan ukuran *eror* dari transmisi paket data. Berikut adalah standar Packet Loss berdasarkan ITU *(International Communication Union)*

Table 2. Kualitas *Packet Loss*

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

Berikut adalah rumus untuk menghitung Packet Loss :

$$\text{Packet Loss} = \frac{\text{P. Data yang dikirim} - \text{P. Data yang diterima}}{\text{Paket Yang Dikirim}} \text{ X } 100\%$$

c. *Throughput*
Throghput merupakan kecepatan rata rata data dalam selang waktu tertentu. Berikut adalah standar Packet Loss berdasarkan ITU *(International Communication Union)*

Table 3. Kualitas *Throughput*

Kualitas Throughput	Throughput
Sangat Bagus	100
Bagus	75
Cukup	50
Buruk	<25

Berikut adalah rumus untuk menghitung *Throughput :*

$$\text{Throughput} = \frac{\text{Jumlah Data yang Dikirim}}{\text{Waktu Pengiriman Data}}$$

d. *Jitter*
Jitter disebabkan karna bervariasinya waktu pengiriman packet data sampai ke penerima .Semakin besar nilai *jitter*, maka nilai Qos akan semakin rendah. Berikut adalah standar Jitter berdasarkan ITU *(International Communication Union)*

Table 4. Kualitas *Jitter*

Kategori Jitter	Besar Jitter
Baik	0 - 20 ms
Cukup	20 - 50 ms
Buruk	>50 ms

Untuk mendapatkan nilai Qos yang baik, maka *jitter* harus seminimum mungkin. Berikut adalah rumus untuk menghitung nilai *Jitter*

$$\text{Jitter} = \frac{\text{Total Variasi delay}}{\text{total Paket Yang Diterima} - 1}$$

Protokol VoIP

Protokol jaringan yang digunakan untuk mengimplementasikan VoIP meliputi :

a. H.323
   Protokol H.323 merupakan suatu standar ITU-T *(International Telecomunications Union – Telecomunications)* yang menentukan komponen protokol, dan prosedur yang menyediakan layanan komunikasi multimedia, yaitu komunikasi audio, video dan data *real-time* (waktu nyata), melalui jaringan berbasis paket *(packet-based network).*
b. *Media Gateway Control Protocol (MGCP)*
   MGCP ialah protokol yang digunakan untuk *signaling* dan *call control* yang digunakan dalam sistem VoIP yang terdistribusi.
c. *Session Initiation Protocol (SIP)*
   SIP merupakan signaling protocol, banyak digunakan untuk membangun dan memutus sesi komunikasi multimedia seperti panggilan suara dan video melalui internet. Protokol ini dapat digunakan untuk membuat, mengubah dan mengakhiri sesi *unicast* atau *multicast* yang terdiri dari satu atau beberapa *media stream.*
d. *Real-time Transport Protocol (RTP)*
   Real-time Transport Protocol (RTP) didefinisikan sebagai standarisasi paket untuk mengirimkan audio dan video pada jaringan IP. RTP digunakan untuk komunikasi dan sistem entertain yang termasuk didalamnya streaming media seperti *telepony*, aplikasi *video teleconfrence* dan web yang memiliki fitur berbasis *push-to-talk.*
e. *Session Description Protocol (SDP)*
   Session Description Protocol adalah sebuah protokol yang mempunyai fungsi untuk memberikan deskripsi terhadap suatu sesi multimedia. Secara umum, protocol SDP digunakan pada saat melakukan *session announcement* serta *session invitation*. Informasi yang diberikan oleh sebuah pesan SDP antara lain adalah nama *session* dan tujuan penggunaan *session,* waktu aktif dari sebuah session, jenis media yang digunakan (audio,video), format media (3GP, MPEG4 ,dsb) dan informasi untuk menerima media tersebut (alamat, port).

VPN *(Virtual Private Network)*

Virtual Private Network atau biasa disebut VPN adalah Sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. VPN merupakan koneksi virtual yang bersifat *private*, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan virtual, dan jaringan tersebut tidak semua orang dapat mengaksesnya sehingga sifatnya *private*. (Oktivasari & Utomo, 2016).

1. Fungsi utama VPN
   Teknologi VPN menyediakan beberapa fungsi utama bagi penggunanya, diantaranya :
   a. *Confidentially* (kerahasiaan)
      Inti utama dari penyadapan ini adalah usaha untuk menjaga informasi dari orang – orang yang tidak berhak mengakses. *Privacy* lebih kearah data – data yang sifatnya prifat. Serangan terhadap aspek *Privacy* misalnya usaha untuk melakukan peyadapan.
   b. *Data integrity* (Keutuhan Data)
      Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya *virus, trojan house*, atau pemakai alat lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.
   c. *Origin Autenthication* (Autentikasi Sumber)
      Untuk menguji identitas dari perusahaan lain yang hendak melakukan transaksi.
   d. *Non- Repudiation*

Untuk mencegah adanya kecurangan di antara salah satu pihak, misalnya tidak mengakui bahwa mereka telah mengirim ataupun menerima sebuah *file*.

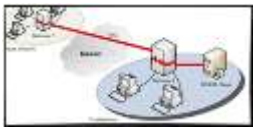
e. Kendali Akses
Bagi yang tidak memiliki hak maka tidak akan bisa mengakses ke jaringan ini.

2. Jenis – jenis Jaringan VPN

a. Access VPN
Access VPN atau Virtual Private Dial-Up Network (VPDN) adalah koneksi *user-to-LAN* yang digunakan untuk koneksi ke jaringan dari berbagai lokasi *remote*. *Remote Access VPN* memungkinkan pekerja untuk mengakses data-data dan segala sumber daya dimanapun mereka berada.

b. Intranet VPN
Intranet VPN atau site to site VPN merupakan VPN yang digunakan untuk menghubungkan antara kantor pusat suatu perusahaan dengan kantor cabang atau kantor pembantu melalui *shared network* menggunakan koneksi yang permanen *(dedicated)*. Tujuan penggunaan intranet VPN agar *administrative control* berada sepenuhnya di bawah satu kendali.

c. Extranet VPN
Extranet VPN merupakan VPN yang digunakan untuk menghubungkan antara kantor dengan pihak luar seperti pelanggan, suplier, rekan bisnis, atau suatu komunitas ke dalam jaringan internal dengan menggunakan *koneksi Dedicated*. Dengan adanya *Extranet VPN* perusahaan-perusahaan yang terlibat dapat berkomunikasi serta bertukar informasi secara cepat, mudah, tapi dalam sistem keamanan yang terjamin.



Gambar 1. Jaringan VPN

Topologi Jaringan

Topologi jaringan adalah salah satu aturan bagaimana menghubungkan komputer (*node*) satu sama lain secara fisik dan pola hubungan antara komponen-komponen yang berkomunikasi melalui media atau peralatan jaringan, seperti *server, workstation, hub/switch,* dan pemasangan kabel (media transmisi data) (Widodo, Yana, & Agung, 2018).

TrixBox

Trixbox adalah sebuah *VoIP server* yang dibuat menjadi satu dengan system operasi yaitu *LINUX Centos*. Trixbox bersifat open source yang artinya setiap orang dapat mengetahui source code programnya dan memperolehnya secara gratis. Trixbox cocok digunakan untuk pengguna rumahan maupun lembaga. Trixbox dapat membuat sebuah jaringan VOIP, melakukan komunikasi jarak jauh, dan jaringan jangkauan pada trixbox luas. (Firmansyah, 2018) . Fungsi TrixBox

Untuk membuat jaringan VoIP , melakukan komunikasi jarak jauh serta berguna untuk jaringan yang luas dan memiliki fitur yang lengkap.

Gambar 2. **Tampilan trixbox**

3CX Phone

3CX Phone adalah aplikasi pendukung VoIP yang memungkinkan untuk mengirim pesan, dan melakukan panggilan suara dan video. (Putra, 2017)

Gambar 3. **Tampilan 3CX Phone**

PEMBAHASAN

Pada tahap ini akan dilakukan implementasi dan penerapan topologi jaringan. Tahap implementasi meliputi konfigurasi server trixbox untuk VoIP konfiurasi OpenVPN, serta konfigurasi 3cx phone pada client.

Konfigurasi VoIP Pada Server Trixbox

Tahap pertama diawali dengan, masuk ke web browser, kemudian ketikkan IP server yang telah di dapat sebelumnya, kemudian setelah muncul tampilan sig in, masuk dan isi username dan password, username : maint dan password : password. Berikut adalah tampilannya :

Gambar 4. Tampilan Admin Trixbox

Berikut adalah tampilan awal trixbox. Masuk ke menu PBX Setting untuk mengakses konfigurasi VOIP.

Gambar 5. Tampilan Trixbox

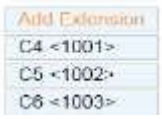
Untuk menambahkan ekstensi dilakukan pada menu *exstension*. pada bagian *device* pilih *generic SIP device* lalu klik *submit.* Isikan *user extension* sebagai nomor telepon dan *display name* sebagai nama pengguna sesuai dengan yang diinginkan.

Gambar 6. *Penambahan Extension*

Gambar 7 *Menu Secret*

Setelah *User* di tambahkan, isikan *password user* pada bagian *menu secret*. Seperti gambar di bawah : Dan berikut adalah tampilan daftar *extension* yang telah di tambahkan

Gambar 8 Tampilan panggilan VOIP



Gambar 9. Daftar Extension

kemudian masuk ke softphone 3CX Phone pilih *setting user* dengan *account name* dapat di sesuaikan, masukan *extension* yang sudah terdaftar pada *trixbox* dan juga *password*. lalu masukan *IP server trixbox* (192.168.1.2)

Gambar 10. Tampilan Setting Account

Selanjutnya, setting user untuk client android , setelah semua sudah terdaftar, kita dapat melakukan panggilan VoIP. Pada aplikasi *zoiper* terlebih dahulu harus diisikan *account name, extension, SIP server, id dan password*. Berikut adalah tampilan *account* pada *zoiper.*

Gambar 11. Tampilan account zoiper

Berikut adalah tampilan ketika akan melakukan panggilan, menggunakan VOIP dan aplikasi *3CX Phone*.

KESIMPULAN DAN SARAN

Kesimpulan

1. System komuniakasi VOIP VPN pada USNI berhasil di buat.
2. QoS (Quality of Service) dari Komunikasi VOIP ini memperoleh nilai delay 7 ms, throughput 25,868 kbps dan packet loss 0 %. Dan kamonukasi VoIP yang telah dibuat tergolong bagus.
3. Dengan menggunakan VPN sebagai keamanan, data yang dikirim melalui VoiP tidak dapat disadap dan direkam.
4. Client yang menggunakan VoIP, harus mendaftar terlebih dahulu pada server Trixbox.
5. Komunikasi VoIP dapat dilakukan jika perangkat yang digunakan terkoneksi dalam satu jaringan.

Saran

Untuk penelitian berikutnya IP Server VPN diharahapkan terkoneksi dengan internet dan dapat menggantikan IP Public agar di kenal global.

DAFTAR PUSTAKA

Azhar, A., Badrul, M., & Akmaludin. (2018, Maret 1). PENERAPAN VOICE OVER INTERNET PTOTOKOL (VOIP) UNTUK OPTIMALISASI JARINGAN PADA BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL. *PENERAPAN VOICE OVER INTERNET PTOTOKOL (VOIP) UNTUK OPTIMALISASI JARINGAN PADA BADAN KEPENDUDUKAN DAN KELUARGA BERENCANA NASIONAL, 5*, 1-8.

Darmawan, I. E. (2016, February). RANCANG BANGUN KEAMANAN TRANSFER DATA VOIP OVER VPN PADA SISTEM OPENSOURCE TRIXBOX. *RANCANG BANGUN KEAMANAN TRANSFER DATA VOIP OVER VPN PADA SISTEM OPENSOURCE TRIXBOX*, 1-11.

Dwiki. (2015, December). Diambil kembali dari http://mydwiki23.blogspot.com/2015/12/definisi-keamanan-jaringan-komputer.html

Firmansyah, F. A. (2018, August 18). Diambil kembali dari https://pembelajaranteknologilayananjaringan.wordpress.com/2018/08/18/mengetahui-pengertian-trixbox-fungsikelebihandan-cara-membuat-topologi-voip-dengan-trixbox-serta-menginstal-trixbox/

Kristalina, P. (2015). VOICE INTERNET OVER PROTOKOL (VOIP) : INTERNET TELEPHONY. *POLITEKNIK ELEKTRONIKA NEGERI SURABAYA*, 1-42.

Oktivasari, P., & Utomo, A. B. (2016, NOVEMBER 30). ANALISA VIRTUAL PRIVAT NETWORK MENGGUNAKAN OVENVPN DENGAN POINT TO POINT TUNNELING PROTOKOL. *POLITEKNIK NEGERI JAKARTA*, 1-18.

Purniasatam. (2017, september 28). Diambil kembali dari https://catataninetkita.wordpress.com/2017/09/28/pentingnya-firewall-dalam-jaringan-komputer/

Purnomo, R. T., & Kurniawan, M. T. (2015, JANUARY 1). ANALISIS DAN DESAIN KEAMANAN JARINGAN KOMPUTER DENGAN METODE NETWORK DEELOPMENT LIFE CYLE (STUDI KASUS: UNIVERSITAS TELKOM). *JURNAL REKAYASA DAN SISTEM INDUSTRI, II*, 1-7.