

Perancangan *Voice Over Internet Protocol* Menggunakan *VPN Gateway-To-Gateway* Berbasis Server

Septian Wahyu Tricahya¹, Agus Prihanto²

^{1,2} Jurusan Teknik Informatika Fakultas Teknik Universitas Negeri Surabaya

¹septian.18077@mhs.unesa.ac.id

²agusprihanto@unesa.ac.id

Abstrak — Keamanan jaringan komunikasi menjadi hal yang perlu diperhatikan di zaman yang sudah serba digital seperti sekarang ini. Banyak aktivitas yang membutuhkan internet sebagai media komunikasi, salah satunya adalah komunikasi untuk kepentingan proses bisnis dalam sebuah perusahaan. Umumnya perusahaan menggunakan jaringan komunikasi dari layanan pihak ketiga yang berpotensi terhadap serangan siber. Ada banyak penyedia layanan komunikasi yang dapat membantu bisnis perusahaan, akan tetapi penyedia layanan tersebut masih memiliki potensi terjadinya serangan siber. Untuk mengatasi hal ini, penggunaan VoIP (*Voice Over Internet Protocol*) dapat menjadi solusi yang tepat untuk meminimalisir terjadinya serangan siber dalam komunikasi bisnis perusahaan. VoIP dapat dimanfaatkan untuk melakukan panggilan telepon serta panggilan video. Hal ini membantu perusahaan agar tetap terhubung dalam kepentingan bisnisnya. Akan tetapi, penggunaan VoIP masih memiliki kerentanan terhadap serangan siber, salah satu serangan yang dapat terjadi adalah penyadapan atau *sniffing*. Maka, perlu adanya teknologi pengamanan pada jaringan yang digunakan perusahaan ketika memilih menggunakan teknologi VoIP. Untuk mengatasi hal ini, penulis akan menggunakan VPN *Point-to-Point Tunneling*, sehingga VoIP akan berjalan di dalam tunnel yang telah dibuat. Hal ini akan meningkatkan keamanan komunikasi perusahaan, bahkan ISP (*Internet Service Provider*) yang digunakan perusahaan tidak akan mengetahui VoIP di dalam VPN yang digunakan. Dengan adanya gagasan ini, peneliti menciptakan suatu rancangan komunikasi VoIP beserta pengamanan melalui sisi jaringan dengan memanfaatkan VPN *Gateway-To-Gateway* dengan tingkat keamanan lebih tinggi serta biaya yang lebih terjangkau.

Kata Kunci — *Voice Over*, VoIP, VPN, *Gateway-To-Gateway*, Server

I. PENDAHULUAN

Keamanan jaringan komputer menjadi hal yang perlu diperhatikan di zaman yang sudah serba digital ini. Hampir semua aktivitas yang membutuhkan internet sebagai media komunikasi, salah satunya adalah aktivitas proses bisnis pada perusahaan besar. Umumnya perusahaan menggunakan jaringan internet biasa yang berpotensi terhadap serangan siber. Perusahaan dapat menggunakan layanan pihak ketiga untuk memenuhi kebutuhan internet perusahaan, akan tetapi hal tersebut memiliki potensi untuk menerima serangan siber. Berdasarkan penelitian yang telah dilakukan oleh Munawar, menjelaskan bahwa jaringan komputer dan teknologi

keamanan terus berkembang, serta teknologi yang digunakan oleh para penjahat kriminal juga mengikuti perkembangan[1].

Pada beberapa kasus serangan siber, umumnya akan menarget keamanan jaringan, sehingga tidak dipungkiri lagi bahwa keamanan jaringan dan aplikasi menjadi hal yang perlu diperhatikan oleh pengembang. Meski demikian, masih ada kemungkinan terdapat celah keamanan yang berhasil ditemukan oleh pihak yang tidak bertanggung jawab. Sebagai contoh, kasus penipuan yang menggunakan teknik *bypass sms* verifikasi menggunakan nomor telepon korban, sehingga celah yang ada bukan dari internal aplikasi VoIP tersebut, melainkan dari jaringan diluar aplikasi VoIP tersebut. Seperti yang telah diungkap oleh Kementerian Komunikasi dan Informatika RI, Direktorat Kejahatan Keras Direktorat Reserse Kriminal Umum Polda Metro Jaya, menyatakan bahwa pelaku tindakan kriminal memanfaatkan VoIP sebagai penipuan online karena susah untuk dikenali, karena VoIP berbeda dengan provider biasa[2]. Hal ini yang menjadi alasan peneliti untuk memanfaatkan kelebihan VoIP guna kepentingan peningkatan keamanan jaringan komunikasi yang dapat digunakan oleh perusahaan.

Pada umumnya, penyedia layanan VoIP akan mengenai biaya berlangganan, dan tidak semua layanan VoIP menyediakan pembayaran di muka. Biaya yang ditawarkan oleh penyedia layanan VoIP juga cukup mahal. Selain itu, biaya yang diperlukan untuk dapat tetap terhubung ke server VoIP juga harus tetap menggunakan transmisi internet umum sebagai media transmisi jaringannya, sehingga data yang melewati jaringan tersebut dapat berpotensi menjadi target *sniffing* oleh pihak yang tidak bertanggung jawab.

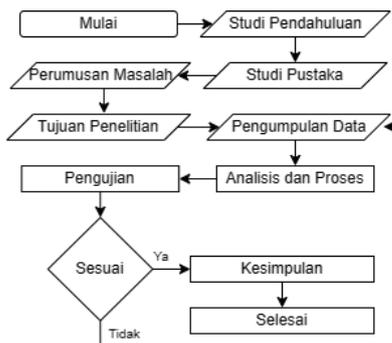
Dengan demikian, peneliti akan memanfaatkan Asterisk sebagai layanan VoIP yang bersifat *opensource*. Tentu menjadi keuntungan perusahaan apabila dibandingkan dengan menggunakan layanan pihak ketiga, baik dari segi biaya serta kemanannya. Asterisk memiliki lisensi yang dapat digunakan oleh siapapun, sehingga dapat dimanfaatkan untuk kepentingan bisnis suatu perusahaan[3]. Selain itu, peneliti juga akan memanfaatkan VPN *Gateway-To-Gateway* dengan tujuan membentuk koneksi yang aman antara dua jaringan yang melalui internet. Dalam hal ini, konfigurasi harus dilakukan pada kedua *router* untuk mengaktifkan VPN *Gateway-To-Gateway*. Konfigurasi yang dilakukan pada bagian *Pengaturan Grup Lokal* dan *Pengaturan Grup Jarak Jauh* harus dibalik antara dua *router*, sehingga grup lokal yang satu adalah grup jarak jauh yang lain. Menurut Dulany, Konfigurasi VPN *Gateway-To-Gateway* dapat digunakan misalnya antara kantor pusat dengan kantor cabang, ataupun antar kantor cabang dengan jarak yang berjauhan[4].

Pada penelitian ini, juga dilakukan tinjauan pustaka guna memperkuat hasil penelitian. Berdasarkan penelitian yang dilakukan oleh Putra dengan judul "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna", peneliti menemukan gagasan untuk membangun sistem keamanan jaringan pada suatu perusahaan dengan berfokus terhadap penggunaan VoIP pada VPN dengan metode protokol PPTP. Peneliti juga akan menggunakan VPN *Gateway-To-Gateway* sebagai media *tunnelling* suara (VoIP) untuk keamanan komunikasi perusahaan.

Gagasan yang digunakan peneliti memiliki keunggulan tersendiri jika dibanding dengan penggunaan aplikasi suara pihak ketiga, seperti biaya yang lebih terjangkau, serta keamanan yang lebih tinggi. Hal ini dikarenakan server dikelola secara langsung oleh perusahaan tanpa campur tangan pihak ketiga. Selain itu, gagasan ini juga memudahkan proses *troubleshooting* apabila terjadi kendala dalam jaringan komunikasi perusahaan.

II. METODOLOGI PENELITIAN

Pada penelitian ini, penulis telah menyusun alur penelitian guna mempermudah proses penelitian. Alur penelitian ini dapat dilihat pada gambar di bawah ini.



Gambar 1 Alur Penelitian

A. Skema Alur Penelitian

1. Studi Pendahuluan

Pada bagian ini, peneliti melakukan studi literatur dengan mendapatkan referensi yang relevan guna memperkuat teori yang digunakan. Di bagian ini, peneliti hanya perlu mencari referensi yang relevan dengan topik penelitian.

2. Studi Pustaka

Pada bagian ini, peneliti melakukan proses pengumpulan data referensi, serta penulisan atau kegiatan awal dari proses pencocokan, pengumpulan data sementara, referensi dari data-data yang diolah untuk melakukan penelitian, semua ini diambil dari buku-buku yang terkait, kutipan mengenai PPTP dan VoIP yang diambil dari internet.

3. Perumusan Masalah

Dari beberapa studi pustaka dan pendahuluan yang telah digagas oleh penulis, serta melakukan observasi terhadap masalah yang terjadi di zaman seperti sekarang, maka penulis mendapat rumusan masalah yaitu *bagaimana cara melakukan komunikasi suara antar kantor cabang perusahaan yang aman dan murah?*

4. Tujuan Penelitian

Dari perumusan masalah yang dapat diambil diatas maka diperoleh tujuan dari penelitian ini yaitu membangun komunikasi VoIP di atas jaringan VPN antar kantor cabang perusahaan dengan menggunakan metode VPN *Gateway-To-Gateway* Server.

5. Pengumpulan Data

Pengumpulan data yang dimaksudkan di sini adalah bagaimana proses pengumpulan semua data dari referensi daftar pustaka dan juga kebutuhan apa saja yang dibutuhkan pada sistem.

6. Analisis dan Proses

Analisa merupakan proses di mana sistem VoIP menggunakan VPN *Gateway-To-Gateway* akan bekerja dan juga berisi tentang prosedur dalam pembuatan sistem.

7. Pengujian

Pengujian hasil analisa yang dilandasi dengan data-data yang telah dikumpulkan serta pengamatan langsung yaitu melakukan pengujian terhadap sistem apakah dapat berfungsi sebagaimana dengan semestinya agar dapat digunakan untuk menarik kesimpulan. Apabila dari pengujian tersebut telah sesuai dengan analisa yang dibutuhkan, maka selanjutnya dapat dijadikan acuan untuk menarik kesimpulan. Namun, jika hasil dari pengujian tidak sesuai maka pengujian tersebut harus diulang pada proses pengumpulan data.

8. Kesesuaian

- Apakah Penulis dapat membangun sistem voip dengan menggunakan VPN *Gateway-To-Gateway* berbasis server?
- Apakah Penulis dapat membangun Virtual Private Network *Gateway-To-Gateway*?

9. Kesimpulan

Setelah pengujian tersebut telah sesuai dengan analisa yang dibutuhkan maka selanjutnya tahap terakhir menarik kesimpulan. Kesimpulan berhubungan erat dengan rumusan masalah yang telah dibuat pada Bab I.

B. Analisa Sistem

Sistem VoIP yang menggunakan VPN *Gateway-To-Gateway* dapat berfungsi dengan baik jika data yang dilewatkan untuk sampai pada alamat tujuan mengalami pembungkusan data guna menciptakan keamanan untuk terhidar dari serangan siber seperti *sniffing*. Dengan

menggunakan perintah *tracert* (pada DOS *prompt*) dan *traceroute* (pada terminal Linux) dapat diketahui proses perjalanan paket sampai pada tujuan. *User* dapat melakukan dan menerima panggilan dengan kualitas suara yang baik.

C. Perancangan Sistem

1. Kebutuhan Hardware

Kebutuhan *hardware* dari perancangan sistem VoIP yang akan peneliti lakukan adalah sebagai berikut:

- Dua buah komputer yang dipergunakan sebagai gateway masing masing kantor cabang dan pada salah satu komputer dijadikan sebagai server VoIP dengan spesifikasi sebagai berikut:
 - Processor Intel Core 2 Duo
 - RAM 4 GB
 - Hardisk 80 GB
 - LAN Card @2 buah
- Headset yang dilengkapi *microphone* (untuk *client*)
- Dua buah router sebagai gateway ke internet
- Kabel LAN

2. Kebutuhan Software

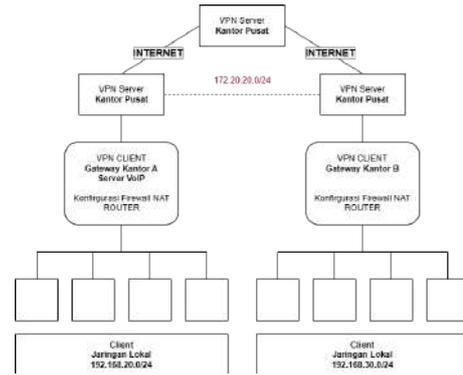
Selain beberapa kebutuhan *hardware* yang telah disebutkan tadi, ada beberapa kebutuhan lain yang harus disediakan dalam perancangan VoIP ini, yaitu sebagai berikut:

- Sistem Operasi Linux Ubuntu 16.04
- Asterisk
- SIP Phone dan MicroSIP

3. Desain Jaringan

Desain sistem VoIP menggunakan VPN *Gateway-To-Gateway* ini terdiri dari empat buah komponen utama yang saling berhubungan, yaitu VoIP server, VoIP *client*, VPN server, VPN *client* dan membutuhkan dua buah perangkat komputer sebagai server. Pada masing masing komputer terdapat salah satu dari komputer tersebut yang dijadikan sebagai VoIP Server.

VoIP server merupakan server untuk pusat penanganan proses, registrasi dan panggilan VoIP *client*. VPN server merupakan server yang digunakan untuk pelayanan jalur komunikasi SIP yang lebih aman. Penggunaan VPN server ini secara fisik menjadi satu dengan VoIP server. Namun pada penelitian ini VPN server hanya digunakan sebagai *bridge* saja karena terkendala biaya oleh penulis. Namun daripada itu tidak mengurangi kualitas penelitian ini.



Gambar 2 Topologi Jaringan VPN

Pada gambar tersebut terdapat beberapa pendukung VoIP yaitu pada jaringan lokal yang dipergunakan sebagai *client* menggunakan alamat IP 192.168.20.0/24. Kemudian pada komputer gateway kantor a terpasang dua buah lan *ethernet* yang masing-masing *port* memiliki IP berbeda, untuk *port ethernet* pertama menggunakan IP Publik yang bersifat dinamis dari ISP penyedia layanan internet, untuk *port ethernet* yang kedua menuju ke jaringan lokal yang nantinya digunakan sebagai gateway oleh *client* pada jaringan lokal pertama.

Pada server B juga terpasang dua buah *port ethernet* yang memiliki alokasi IP Publik dinamis dari ISP penyedia layanan dan untuk yang kedua memiliki alokasi IP 192.168.30.0 yang dipergunakan sebagai gateway oleh *client*.

Selain memiliki *port ethernet* fisik pada masing-masing komputer gateway, juga terpasang *device ethernet card virtual* yang nantinya *ethernet* tersebut dipergunakan sebagai jalur komunikasi melalui terowongan oleh VPN. Alokasi IP yang digunakan tentunya harus berbeda dengan *ethernet* fisik yang tersedia agar menghindari terjadinya konflik jaringan. Untuk alokasi IP yang dipergunakan yaitu 172.20.20.2 untuk komputer gateway pertama dan 172.20.20.3 untuk gateway komputer yang kedua.

Pada saat komputer masing-masing gateway bekerja, masing-masing komputer gateway akan melakukan NAT semua jaringan yang melalui gateway tersebut. Termasuk saat VPN tersebut diaktifkan, maka semua trafik yang ada pada jaringan lokal akan dibelokkan ke jaringan VPN. Karena agar dapat berkomunikasi antar klien harus menggunakan jaringan sama tanpa ada nya VPN, maka klien tidak dapat ditembus melalui NAT atau dengan kata lain IP Publik tidak dapat berkomunikasi dengan IP Private, maka dari itu perlu adanya *tunnelling* pada masing-masing jaringan agar dapat bertemu menjadi satu jaringan.

4. Perancangan Gateway Kantor

Bagian ini peneliti akan menjelaskan tahapan dalam melakukan konfigurasi dan perancangan pada server A. Alasan utama tidak menggunakan *openvpn* karena konfigurasi VPN PPTP lebih mudah dan hampir semua sistem operasi sudah mendukung dan tersedia layanan VPN

PPTP, selain itu dengan menggunakan *openvpn*, diperlukan IP Public dan IP Transit yang cukup susah untuk dikonfigurasi. Di mana alur konfigurasi dapat dilihat pada gambar di bawah ini:



Gambar 3 Alur Konfigurasi Server

5. Setting IP Address dan Gateway

Pada komputer server yang pertama terdapat dua *port ethernet* yang secara otomatis penamaan oleh Linux dengan nama *enp1s0* dan *enp3s0*. Untuk mengatur IP pada *port ethernet* pertama dapat dilakukan melalui konfigurasi pada file yang terdapat pada direktori */etc/network/interfaces*.

```
seps@seps:~$ nano /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto enp0s8
iface enp0s8 inet static
    address 192.168.20.2/24 # IP Address
    gateway 192.168.20.1/24 # Gateway
    dns-nameservers 8.8.4.4 # DNS Address
```

Gambar 4 Konfigurasi IP Server

Selanjutnya, mengaktifkan firewall dengan perintah *sudo ufw enable* hingga muncul notifikasi “Firewall is active and enabled on system startup”. Jika *firewall* berhasil diaktifkan, maka dapat dilanjutkan ke langkah berikutnya yaitu mengkonfigurasi IPv4 *Forwarding* dengan menghapus tanda pagar (#) pada kode *net/ipv4/ip_forward=1* yang terdapat dalam file */etc/ufw/sysctl.conf*

Dari sini sebetulnya jaringan sudah dapat dilewatkan dari *client* namun perlu adanya konfigurasi untuk mengizinkan jaringan yang lewat demi alasan keamanan dengan menambahkan kode *iptables -P INPUT ACCEPT* pada file dalam direktori */etc/rc.local*. Penambahan kode tersebut ke dalam file *rc.local* bertujuan untuk meningkatkan efisiensi, hanya dengan menjalankan perintah *sudo chmod 755 /etc/rc.local* maka penambahan kode pada file *rc.local* tadi dapat berjalan otomatis ketika server dinyalakan atau di-restart.

Setelah kedua *port ethernet* dilakukan konfigurasi IP dan Gateway, maka selanjutnya adalah melakukan tes koneksi. Namun, sebelum melakukan tes koneksi pada masing masing *port ethernet*, perlu dicek terlebih dahulu apakah konfigurasi dari masing-masing *port* sudah berhasil

atau belum, dengan menjalankan perintah *ifconfig <nama Ethernet>*.

```
seps@seps:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:3b:e7:4e
    inet 192.168.20.132 netmask 255.255.0.0 broadcast 192.168.20.255
    inet6 fe80::2090:1b0c:6f0d:ab77:64 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:127 errors:0 dropped:0 overruns:0 frame:0
    TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:22071 (22.0 KB)  TX bytes:14058 (14.0 KB)

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:35:ef:e5
    inet 192.168.20.2 netmask 255.255.0.0 broadcast 192.168.20.255
    inet6 fe80::a00:27ff:fe35:efe5:04 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:132 errors:0 dropped:0 overruns:0 frame:0
    TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:2290 (2.3 KB)  TX bytes:9379 (9.3 KB)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1:1:1:1:1:1:1:1 Scope:Host
    UP LOOPBACK RUNNING  MTU:65536  Metric:1
    RX packets:35 errors:0 dropped:0 overruns:0 frame:0
    TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:2457 (2.4 KB)  TX bytes:2457 (2.4 KB)
```

Gambar 5 Menjalankan perintah Ifconfig

Dari *output* pada gambar di atas, menunjukkan bahwa *port ethernet* pertama yaitu *enp0s3*. Pada *port* tersebut mengarah ke ISP, *port ethernet* menggunakan IP Dinamis, karena pada dasarnya IP yang diberikan oleh ISP bersifat dinamis, maka dari itu tidak perlu adanya konfigurasi IP dan *gateway* pada *port* tersebut. Sedangkan *port ethernet* *enp0s8* mengarah ke klien dengan konfigurasi IP dan *gateway* sebagai berikut untuk ip dari *port* tersebut menggunakan jaringan 192.168.20.2.

```
seps@seps:~$ ip route
default via 192.168.20.2 dev enp0s3 proto static metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.20.0/24 dev enp0s8 proto kernel scope link src 192.168.20.2
192.168.20.0/24 dev enp0s3 proto kernel scope link src 192.168.20.132
```

Gambar 6 Melihat Rute Jaringan

Dari konfigurasi yang telah dilakukan, langkah selanjutnya yaitu menentukan arah paket yang akan dibawa, dengan menjalankan perintah *ip route -n* untuk melihat rute dari semua jaringan yang terdapat pada Linux. Selain itu, *route* pada linux sangat penting karena linux dilewati oleh jaringan client. Dari konfigurasi yang dilakukan peneliti, semua trafik jaringan diarahkan menuju ke internet melalui *ethernet 1* atau *enp0s3* dengan IP yang diperoleh bersifat dinamis dari *router* IP. Untuk melihat apakah jaringan client terhubung ke internet maka dapat dibuktikan dengan melakukan ping, dan hasil ping ke alamat IP 8.8.4.4 dengan waktu 22.8 millisecond yang berarti jaringan terhubung ke internet dengan baik. Ini merupakan langkah awal yang harus dipenuhi dalam menjalankan perintah selanjutnya. Karena pada penelitian kali ini membutuhkan jaringan internet sebagai transmisi/jalur yang dipergunakan untuk berkomunikasi.

6. Konfigurasi VPN Point to Point Tunneling

Konfigurasi ini sangat mudah karena tidak perlu adanya instalasi seperti VPN lainnya, karena VPN PPTP sudah tersedia dari Linux. Langkah selanjutnya yaitu tinggal memasukan *host/alamat* VPN yang telah dibuat. Dalam penelitian ini, server yang digunakan adalah server dari Universitas negeri Surabaya yang diasumsikan sebagai

kantor pusat, sehingga pada konfigurasi ini berfokus pada konfigurasi pada segi klien.

- a. Membuat jaringan VPN PPTP, langkah ini dimulai dengan menambahkan adapter baru di Network Connections, lalu menambahkan koneksi VPN, hingga menghubungkan ke VPN yang telah dibuat.
- b. Instalasi Asterisk, proses instalasi Asterisk dapat dilakukan dengan cara sebagai berikut:
 - 1.) Update sistem Linux dengan perintah `sudo apt update`
 - 2.) Install `build essential` dengan perintah `sudo apt install build-essential`
 - 3.) Install dependensi yang dibutuhkan dengan perintah `sudo apt-get install git-core subversion wget libjansson-dev sqlite autoconf automake libxml2- dev libncurses5-dev libtool`
 - 4.) Setelah itu, masuk ke dalam direktori `/usr/src/`, dan jalankan perintah `sudo wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-16-current.tar.gz`
 - 5.) Setelah itu lakukan ekstraksi dengan perintah `wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-14-current.tar.gz`
 - 6.) Install Asterisk yang sudah diekstrak dengan perintah `./configure`

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

1. Perbandingan Penganggaran

Pada penelitian ini telah dijelaskan bahwasanya penelitian ini memiliki alokasi anggaran yang lebih murah dan aman dibanding menggunakan pihak lainnya selain itu pada aspek perawatan juga lebih efisien dan juga tidak perlu biaya berlangganan. Berikut merupakan rincian pengalokasian anggaran pada penelitian ini:

Tabel 1 Harga Server Lokal

No	Nama	Harga (Rp)	Jumlah	Total (Rp)
1.	Komputer	800.000	2 pcs	1.600.000
2.	Monitor	500.000	2 pcs	1.000.000
3.	Mouse	35.000	2 pcs	70.000
4.	Keyboard	50.000	2 pcs	100.000
5.	Kabel LAN	370.000	305m	370.000
6.	RJ45	16.000	1 pck	16.000
7.	Router	200.000	2 pcs	400.000
8.	Perawatan oleh Karyawan	2.000.000	1 orang	2.000.000
Total				5.556.000

Pada rincian alokasi anggaran tersebut diluar kebutuhan pokok ISP. Karena pada perbandingan antara penelitian ini dan pihak ketiga sama sama menggunakan ISP sebagai kebutuhan internetnya. Pada perancangan ini

dapat mengeluarkan anggaran sejumlah Rp 5.556.000 dibanding dengan penggunaan biaya ketiga selain factor keamanan juga mempertimbangkan faktor biaya yang dikeluarkan berlangganan.

Tabel 2 Harga Layanan VoIP

No	Layanan	Biaya (Rp)
1.	Zoom VoIP	2.400.000/Tahun/Pengguna
2.	RingCentral	10.960.260/Tahun/Pengguna
3.	CouldTalk	8.700.000/Tahun/Pengguna
4.	Telkom	2.340.000/3 Jam Panggilan/Pengguna

Pada Biaya Berlangganan Telkom Berbeda dengan biaya berlangganan lainnya. Pada VoIP lainnya umumnya menggunakan biaya tunggal yang disediakan namun untuk penyedia layanan Telepon Interlokal (Jarak 30km – 200 km) milik Telkom memiliki rincian sebagai berikut:

- a. 6 Detik = Rp 1375
- b. 60 detik : 60 Detik = Rp 1374 x 10 = Rp 13.740 / 1 Menit
- c. 1 Menit x 60 Menit = Rp 13.740 x 60 = Rp 824.400 / 60 Menit
- d. 3 Jam = Rp 2.473.200

Pada rincian diatas diasumsikan perusahaan melakukan panggilan setiap hari maks hanya 3 jam jika di rata rata tiap harinya. Dari data tabel yang didapat harga di ambil per tanggal 17 Nov 2022 menunjukkan bahwa harga VoIP masih tinggi pada segi bisnis. Selain itu juga dengan menggunakan penelitian ini selain harga yang cukup murah juga lebih mudah untuk perawatannya. Karena server berada dan dikelola oleh perusahaan itu sendiri.

2. Keamanan VPN PPTP

Dapat dikatakan aman tentu perlu adanya pembuktian berupa data yang valid dan dapat dipercaya, pada penelitian ini berfokus pada Rancang Bangun sehingga data yang diperoleh dari penelitian ini mengacu pada artikel yang telah dibuat dan diteliti sebelumnya oleh Jupriyadi yang berjudul “Analisis Keamanan Voice Over Internet Protocol (VOIP) Menggunakan PPTP dan ZRTP”, dari jurnal tersebut, peneliti melakukan pengujian dengan cara melakukan *sniffing* paket menggunakan aplikasi Wireshark[5].

Pada pengujian pertama penguji melakukan pengujian VoIP tanpa pengaman menunjukkan hasil. Hal ini berarti bahwa paket VoIP berhasil di-capture oleh peretas atau pihak ketiga dalam jaringan tersebut, dalam percakapan tersebut hampir mampu didengar ulang dengan jelas percakapan yang dilakukan melalui VoIP tanpa pengaman.

Percobaan kedua dilakukan dengan menggunakan pengaman. Pengaman pada percobaan kedua menggunakan VPN PPTP. Pada percobaan kedua percakapan tidak ditemukan atau tidak terdeteksi oleh aplikasi Wireshark yang diasumsikan sebagai peretas. Dalam proses *sniffing*

yang dilakukan menunjukkan bahwa tidak ada aktifitas yang sedang berlangsung meskipun sebenarnya VoIP sedang berlangsung, hal ini dikarenakan penggunaan pengamanan PPTP.

Hasil perbandingan dari kedua aktivitas tersebut adalah sebagai berikut:

Tabel 3 Hasil Perbandingan VoIP

Pengujian	Capture	
	Deteksi VoIP	RTP Stream
VoIP	Terdeteksi	Terdeteksi
VoIP dengan ZRTP	Terdeteksi	Tidak Terdeteksi
VoIP dengan VPN PPTP	Tidak Terdeteksi	Tidak Terdeteksi

B. Pengujian

1. IP Address dan Gateway

Untuk mengkonfigurasi setiap port ethernet yang tersedia dapat dilakukan dengan cara membuka file yang ada pada directory `/etc/network/interfaces`.

```

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto enp0s8
iface enp0s8 inet static
    address 192.168.20.2/24
    gateway 192.168.20.1/24
    dns-nameservers 8.8.4.4
    
```

Gambar 7 Konfigurasi IP Server

Dalam penelitian ini, penulis menentukan bahwa IP yang mengarah menuju local adalah 192.168.20.2/24 dengan gateway 192.168.20.2/24, sedangkan pada port eth0/enp0s3 mengarah menuju ISP sengaja dikosongkan karena menggunakan IP DHCP yang didapat dari router ISP.

Setelah melakukan konfigurasi IP Linux, maka akan dapat terhubung dengan jaringan internet namun Linux tidak dapat membagi jaringan dengan klien di bawahnya, demi alasan keamanan maka dari itu perlu ada nya konfigurasi NAT pada masing masing Linux.

2. Tes Koneksi

Untuk melihat hasil koneksi dari setiap adapter yang telah dikonfigurasi, dapat dilakukan menggunakan perintah `ifconfig` untuk menampilkan semua adapter atau `ifconfig <nama adapter>` untuk menampilkan adapter tertentu. Beberapa informasi akan terlihat pada terminal server. Terdapat dua adapter ethernet yang tersedia. Adapter ini dapat bertambah jika koneksi VPN diaktifkan.

Untuk melihat hasil konfigurasi gateway yang telah dilakukan sebelumnya serta untuk mengetahui rute yang dilewati jaringan tersebut, dapat dilakukan dengan cara mengetik perintah berikut `route -n`.

```

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.28.2 0.0.0.0 UG 100 0 0 enp0s3
192.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
192.168.20.0 0.0.0.0 255.255.255.0 U 6 0 0 enp0s8
192.168.28.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
    
```

Gambar 8 Melihat Route Jaringan

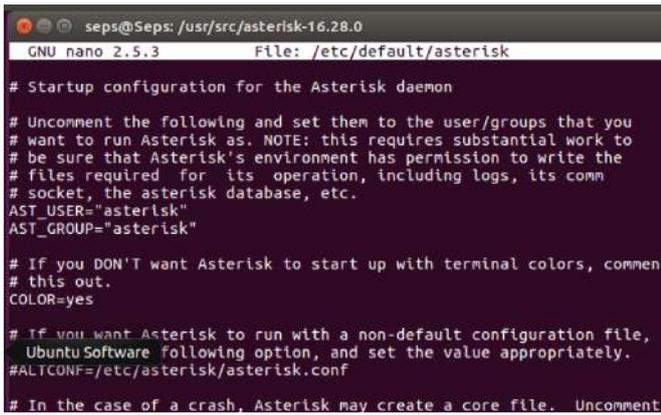
Pada gambar di atas, tertulis alamat IP yang ada yaitu 0.0.0.0, ini bermaksud alamat IP default atau semua jaringan yang ada pada komputer tersebut. Semua komputer yang terdapat pada komputer server tersebut diarahkan menuju ke IP 192.168.28.2 termasuk jaringan klien yang ada di bawahnya akan di NAT atau di *masquerade* alamat IP tersebut. Jadi jaringan yang ada di atas komputer tersebut mengetahui alamat tersebut. Untuk melakukan pembuktian apakah server telah terhubung dengan alamat 192.168.28.2 maka dapat dilakukan dengan metode ping menuju alamat tersebut. Seperti pada gambar dibawah ini.

3. Instalasi Asterisk

Seperti yang telah dijelaskan sebelumnya, Asterisk merupakan software IP PBX untuk membuat sistem layanan komunikasi telepon melalui internet atau biasa disebut VoIP. Asterisk sangat banyak karena Asterisk bersifat *opensource* sehingga pengembang dapat leluasa mengembangkan SIP dengan Asterisk ini. Beberapa syarat yang harus dipenuhi dalam menginstall Asterisk adalah menggunakan operasi sistem Ubuntu yang terbaru dan memiliki akses ke ssh root ke server host terkait. Dalam hal ini yang bertugas sebagai host adalah kantor pusat yang memiliki IP Public dan sebagai host seluruh kantor cabang yang ada di bawahnya.

Di bagian Metode Penelitian telah dijelaskan prosedur instalasi Asterisk, setelah proses instalasi selesai maka langkah selanjutnya adalah konfigurasi Asterisk serta nama pengguna yang nanti akan dapat saling berkomunikasi. Langkah-langkahnya adalah sebagai berikut:

- Masuk ke dalam direktori Asterisk.
- Lakukan konfigurasi sampel dengan perintah `sudo make samples`.
- Buat config dengan perintah `sudo make config` lalu `sudo ldconfig`.
- Melakukan setting non-root untuk Asterisk dengan perintah `sudo groupadd asterisk`.
- Melakukan konfigurasi lokasi user Asterisk dengan perintah `sudo adduser --system --group --home /var/lib/asterisk --no-create-home --gecos "Asterisk PBX" asterisk`.
- Menambahkan Dialout dan Audio dengan perintah `sudo usermod -a -G dialout,audio asterisk`.
- Modifikasi file agar nama pengguna terdeteksi oleh Asterisk dengan perintah `sudo nano /etc/default/asterisk`.



```
seps@Seps: /usr/src/asterisk-16.28.0
GNU nano 2.5.3 File: /etc/default/asterisk

# Startup configuration for the Asterisk daemon

# Uncomment the following and set them to the user/groups that you
# want to run Asterisk as. NOTE: this requires substantial work to
# be sure that Asterisk's environment has permission to write the
# files required for its operation, including logs, its comm
# socket, the asterisk database, etc.
AST_USER="asterisk"
AST_GROUP="asterisk"

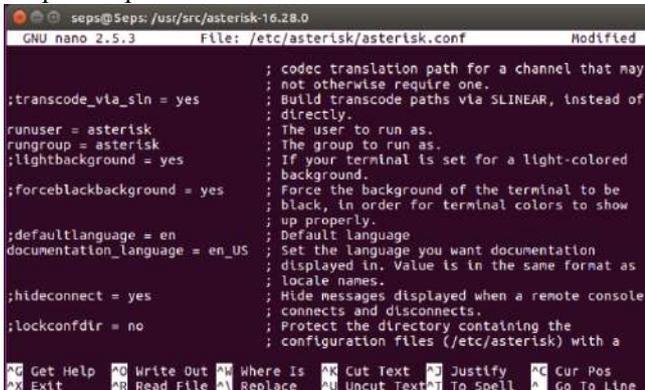
# If you DON'T want Asterisk to start up with terminal colors, commen
# this out.
COLOR=yes

# If you want Asterisk to run with a non-default configuration file,
# Ubuntu Software following option, and set the value appropriately.
#ALTCNF=/etc/asterisk/asterisk.conf

# In the case of a crash, Asterisk may create a core file. Uncomment
```

Gambar 9 Pengaktifan Izin User Asterisk

Terlihat pada file `sudo nano /etc/default/asterisk` ada beberapa baris yang masih terdapat simbol komen yang artinya perintah tersebut belum berjalan. Untuk mengaktifkan dari perintah dari file tersebut dengan cara menghilangkan tanda pagar (#) pada awal baris tersebut. Pada informasi tersebut dapat terlihat untuk `AST_USER="asterisk"` dan `AST_GROUP="asterisk"` sudah berhasil dihilangkan untuk tanda pagarnya. Yang artinya fungsi ini telah berhasil di enable. Meskipun pada file tersebut berhasil dihilangkan centangnya atau berhasil di enable. Bukan berarti fungsi tersebut dapat berjalan dengan lancar ada beberapa nama pengguna yang harus diaktifkan lagi. Untuk mengaktifkannya dapat dibuka dengan perintah `sudo nano /etc/asterisk/asterisk.conf`, maka akan terbuka tampilan seperti berikut:

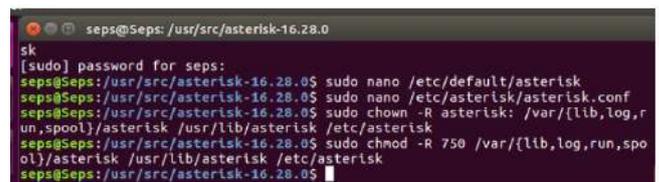


```
seps@Seps: /usr/src/asterisk-16.28.0
GNU nano 2.5.3 File: /etc/asterisk/asterisk.conf Modified

; codec translation path for a channel that may
; not otherwise require one.
; Build transcode paths via SLINEAR, instead of
; directly.
runuser = asterisk
; The user to run as.
rungroup = asterisk
; The group to run as.
;lightbackground = yes
; If your terminal is set for a light-colored
; background.
;forceblackbackground = yes
; Force the background of the terminal to be
; black, in order for terminal colors to show
; up properly.
;defaultlanguage = en
; Default language
documentation_language = en_US
; Set the language you want documentation
; displayed in. Value is in the same format as
; locale names.
;hideconnect = yes
; Hide messages displayed when a remote console
; connects and disconnects.
;lockconfdir = no
; Protect the directory containing the
; configuration files (/etc/asterisk) with a
```

Gambar 10 Menjalankan Akses Khusus

Dapat terlihat pada halaman tersebut pada fungsi lainnya semua fungsi masih belum diaktifkan untuk mengaktifkan fungsi tersebut dengan cara menghilangkan tanda titik koma (;) pada setiap awalan fungsi. Langkah selanjutnya yaitu merubah hak akses dari asterisk yang telah dibuat dengan cara memasukkan perintah seperti berikut:



```
seps@Seps: /usr/src/asterisk-16.28.0
[sudo] password for seps:
seps@Seps: /usr/src/asterisk-16.28.0$ sudo nano /etc/default/asterisk
seps@Seps: /usr/src/asterisk-16.28.0$ sudo nano /etc/asterisk/asterisk.conf
seps@Seps: /usr/src/asterisk-16.28.0$ sudo chown -R asterisk: /var/{lib,log,r
un,spool}/asterisk /usr/lib/asterisk /etc/asterisk
seps@Seps: /usr/src/asterisk-16.28.0$ sudo chmod -R 750 /var/{lib,log,run,spo
ol}/asterisk /usr/lib/asterisk /etc/asterisk
seps@Seps: /usr/src/asterisk-16.28.0$
```

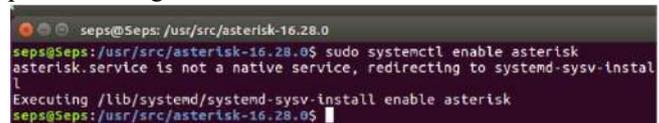
Gambar 11 Merubah Hak Akses

Dengan memasukkan perintah berikut, maka hak akses sudah berhasil diganti:

```
sudo chown -R asterisk:
/var/{lib,log,run,spool}/asterisk
/usr/lib/asterisk /etc/asterisk

sudo chmod -R 750
/var/{lib,log,run,spool}/asterisk
/usr/lib/asterisk /etc/asterisk
```

Sampai disini configure dari asterisk sudah berhasil. Untuk melakukan cek terhadap layanan asterisk yang telah dibuat aktif atau belum maka dapat dibuktikan dengan perintah sebagai berikut:

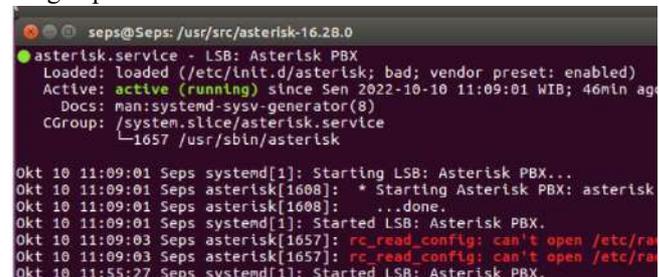


```
seps@Seps: /usr/src/asterisk-16.28.0
seps@Seps: /usr/src/asterisk-16.28.0$ sudo systemctl enable asterisk
asterisk.service is not a native service, redirecting to systemd-sysv-instal
l
Executing /lib/systemd/systemd-sysv-install enable asterisk
seps@Seps: /usr/src/asterisk-16.28.0$
```

Gambar 12 Mengaktifkan Asterisk

Untuk memulai layanan asterisk dapat dijalankan dengan perintah `sudo systemctl start asterisk`.

Maka server asterisk akan berjalan pada linux. Untuk membuktikan status dari asterisk maka dapat dibuktikan dengan perintah berikut:



```
seps@Seps: /usr/src/asterisk-16.28.0
● asterisk.service - LSB: Asterisk PBX
   Loaded: loaded (/etc/init.d/asterisk; bad; vendor preset: enabled)
   Active: active (running) since Sen 2022-10-10 11:09:01 WIB; 46min ago
     Docs: man:systemd-sysv-generator(8)
    CGroup: /system.slice/asterisk.service
           └─1657 /usr/sbin/asterisk

Okt 10 11:09:01 Seps systemd[1]: Starting LSB: Asterisk PBX...
Okt 10 11:09:01 Seps asterisk[1608]: * Starting Asterisk PBX: asterisk
Okt 10 11:09:01 Seps asterisk[1608]:   ...done.
Okt 10 11:09:01 Seps systemd[1]: Started LSB: Asterisk PBX.
Okt 10 11:09:03 Seps asterisk[1657]: rc_read_conf: can't open /etc/ra
Okt 10 11:09:03 Seps asterisk[1657]: rc_read_conf: can't open /etc/ra
Okt 10 11:55:27 Seps systemd[1]: Started LSB: Asterisk PBX.
```

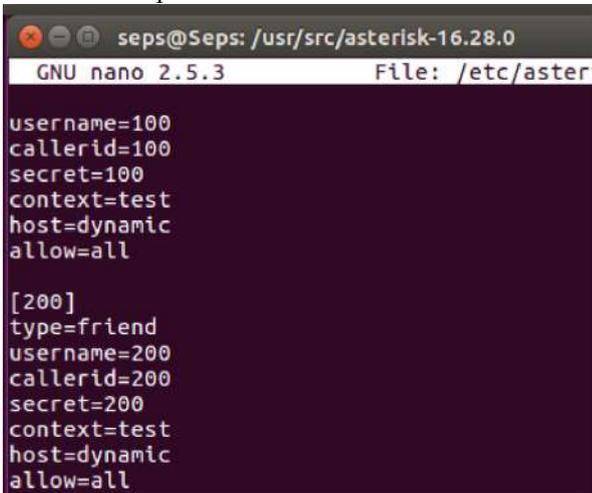
Gambar 13 Melihat Status Asterisk

Pada perintah tersebut dapat dilihat bahwa status asterisk telah aktif dan berjalan pada background. Kemudian untuk masuk pada CLI asterisk dapat dibuktikan dengan perintah `sudo asterisk -rvvv`.

Untuk melakukan komunikasi pada server asterisk tentunya diperlukan konfigurasi pengguna agar dapat terhubung satu pengguna dengan pengguna lainnya. Pada saat berkomunikasi perlu adanya alamat yang harus dituju. Untuk alamat jaringan yang dituju berubah alamat internet protocol (IP) sedangkan untuk alamat dari asterisk berubah nomor yang dapat dibuat dengan bebas. Untuk membuat nomor alamat dari masing-masing pengguna tersebut dapat dibuat

pada server asterisk. Dengan cara mengetikkan perintah **nano /etc/asterisk/users.conf**.

Pada file tersebut berisi konfigurasi lainnya. Untuk menambahkan user dan nomor telepon harus ditambahkan dibawah [general] untuk format penambah pengguna dapat ditambahkan seperti berikut:



```
seps@Seps: /usr/src/asterisk-16.28.0
GNU nano 2.5.3 File: /etc/asterisk/users.conf

username=100
callerid=100
secret=100
context=test
host=dynamic
allow=all

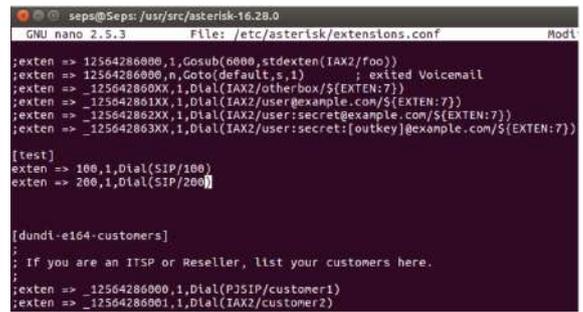
[200]
type=friend
username=200
callerid=200
secret=200
context=test
host=dynamic
allow=all
```

Gambar 14 Menambahkan Username

Pada halaman tersebut merupakan tampilan yang harus diisi untuk pengguna asterisk yang akan didaftarkan. Berikut keterangannya:

- [100] = adalah nama pengguna dan akan menjadi ekstensi di asterisk.
- Type] = untuk menambahkan jenis pengguna apakah teman maupun rekan bisnis.
- [username] = digunakan sebagai nama pengguna yang akan dikenal oleh pengguna lain.
- [Caller ID] = ini merupakan nomor telepon dari pengguna yang juga dapat sebagai alamat pengguna.
- [secret] = merupakan kata sandi dari pengguna ketika login pada aplikasi SIP.
- [context] = hanya sebagai kategori pengguna.
- [Host] = merubakan status untuk memberitahu asterisk bahwa alamat ip yang dimiliki pengguna bersifat dinamis.
- [Allow] = mengizinkan semua codec dijalankan pada asterisk.

Berikut untuk penjelasan keterangan yang tertulis pada konfigurasi pengguna asterisk yang telah dibuat. Langkah selanjutnya yaitu membuat daftar sambungan dari pengguna asterisk yang telah dibuat dengan perintah **nano /etc/asterisk/extensions.conf**, maka akan muncul tampilan seperti berikut:



```
seps@Seps: /usr/src/asterisk-16.28.0
GNU nano 2.5.3 File: /etc/asterisk/extensions.conf

;exten => 12564286000,1,Gosub(6000_stdexten(IAX2/foo))
;exten => 12564286000,n,Goto(default,s,1) ; exited Voicemail
;exten => 12564286000,1,Dial(IAX2/other-box/${EXTEN:7})
;exten => 12564286000,1,Dial(IAX2/user@example.com/${EXTEN:7})
;exten => 12564286200,1,Dial(IAX2/user:secret@example.com/${EXTEN:7})
;exten => 12564286300,1,Dial(IAX2/user:secret:[outkey]@example.com/${EXTEN:7})

[test]
exten => 100,1,Dial(SIP/100)
exten => 200,1,Dial(SIP/200)
```

Gambar 15 Menghubungkan Sambungan

Setelah semua konfigurasi berhasil dibuat langkah selanjutnya yaitu harus melakukan restart pada pengguna yang telah dibuat tadi, agar pengguna asterisk yang telah didaftarkan dapat diketahui oleh asterisk dengan perintah **sudo systemctl restart asterisk**.

Setelah berhasil melakukan restart dengan perintah tersebut. Maka pengguna asterisk sudah berjalan. Untuk melihat pengguna asterisk harus masuk pada sistem CLI dari asterisk tersebut dengan cara mengetik perintah berikut:

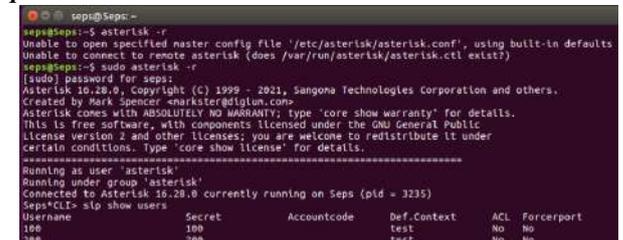


```
seps@Seps: /usr/src/asterisk-16.28.0$ sudo asterisk -rvw
Asterisk 16.28.0, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.

=====
Running as user 'asterisk'
Running under group 'asterisk'
Connected to Asterisk 16.28.0 currently running on Seps (pid = 1657)
seps@CLI>
```

Gambar 16 Masuk ke CLI Asterisk

Langkah selanjutnya yaitu dengan mengetikkan perintah **slip show users**.



```
seps@Seps:~$ sudo asterisk -rvw
Unable to open specified master config file '/etc/asterisk/asterisk.conf', using built-in defaults
Unable to connect to remote asterisk (does /var/run/asterisk/asterisk.ctl exist?)
seps@Seps:~$ sudo asterisk -rvw
[sudo] password for seps:
Asterisk 16.28.0, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.

=====
Running as user 'asterisk'
Running under group 'asterisk'
Connected to Asterisk 16.28.0 currently running on Seps (pid = 3235)
seps@CLI> slip show users
=====
Username      Secret      Accountcode  Def.Context  ACL  Forceport
-----
100           100         test         test         No   No
200           200         test         test         No   No
=====
```

Gambar 17 Melihat Peer User

Terdapat dua pengguna yang aktif dan siap untuk di hubungkan melalui klien asterisk pada jaringan local.

4. Pengaktifan Jaringan Virtual PPTP

Ketika VPN diaktifkan maka semua trafik yang ada pada jaringan tersebut akan berubah ke jaringan VPN tersebut. Secara tidak langsung penggunaan jaringan VPN seolah-olah pengguna berada pada jaringan yang sama meskipun di tempat yang berbeda. Untuk mengaktifkan vpn ini diperlukan server pusat sebagai server dari vpn tersebut. Untuk mengaktifkan VPN PPTP cukup mudah. Berbeda dengan VPN lainnya. VPN PPTP ini sudah tersedia pada linux sehingga ketika ingin menggunakan vpn ini tinggal melakukan konfigurasi pada Linux. setelah melakukan

konfigurasi seperti yang sudah dijelaskan sebelumnya Langkah selanjutnya merupakan mengaktifkan vpn.

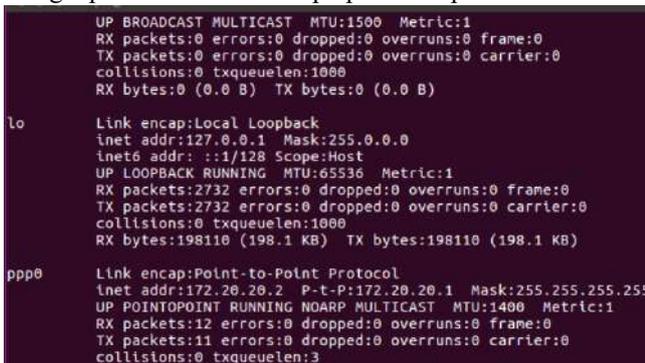


Gambar 18 VPN Berhasil Tersambung

Gambar diatas menunjukkan koneksi VPN sudah terhubung ke server vpn yang ada di kantor pusat. Disisi lain semua jaringan yang ada pada linux tersebut juga sudah dialihkan menuju server pusat vpn sehingga nanti nya pada server pusat tersebut semua jaringan klien dari seluruh kantor cabang akan bertemu tanpa melewati jaringan internet.

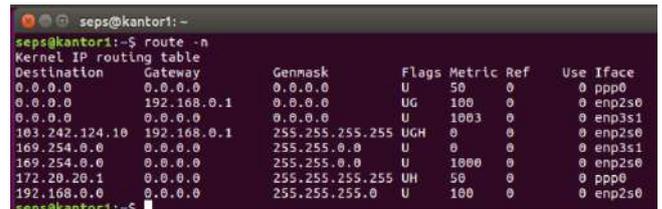
5. Tes Koneksi VPN PPTP

Setelah VPN PPTP dijalankan maka terdapat adapter baru yang akan muncul pada informasi ifconfig hal tersebut sebagai pembuktian bahwa vpn pada komputer telah aktif.



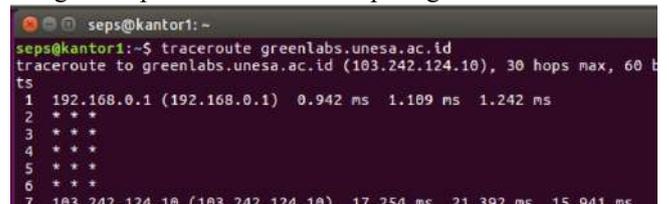
Gambar 19 Ifconfig VPN

Pada informasi tersebut ada beberapa indeks yang menampilkan terkait seluruh informasi dari jaringan yang ada pada komputer server tersebut terlihat pada informasi tersebut inet addr merupakan kata lain dari Internet protocol atau IP. IP yang digunakan pada jaringan tersebut adalah 172.20.20.2 dengan gateway pusat dari vpn tersebut merupakan 172.20.20.1. Gateway 172.20.20.1 merupakan gateway yang terdapat pada komputer pusat dari perusahaan tersebut yang nantinya menjadi gateway pusat yang dapat diakses oleh komputer cabang yang ada dibawahnya. setelah vpn tersebut aktif berarti semua jaringan yang ada di komputer tersebut berubah menjadi satu klas jaringan yang ada di 172.20.0.0.



Gambar 20 Melihat Route

Untuk membuktikan bahwa semua jalur yang terdapat pada jaringan tersebut dapat dilihat dengan mengetikan perintah route -n. informasi ini menampilkan seluruh jalur dari komputer tersebut. Untuk ip yang tampil dengan format 0.0.0.0 merupakan default dari jaringan. Destination merupakan ip tujuan dari jaringan sedangkan gateway adalah ip yang digunakan sebagai pusat jaringan. Pada informasi tersebut pada destination 0.0.0.0 yang artinya semua jaringan tujuan akan keluar menggunakan gateway default pada jaringan. Gateway merupakan ip 192.168.0.1 sesuai dengan yang tertera pada tampilan tersebut. Kemudian pada destination prioritas yang dapat dilihat pada urutan 1 memiliki prioritas tertinggi dengan nama adapter PPP0 yang artinya menggunakan adapter virtual. Untuk membuktikan apakah jaringan sudah melewati terowongan virtual atau belum dapat dibuktikan dengan mengetikan perintah traceroute seperti gambar dibawah ini:

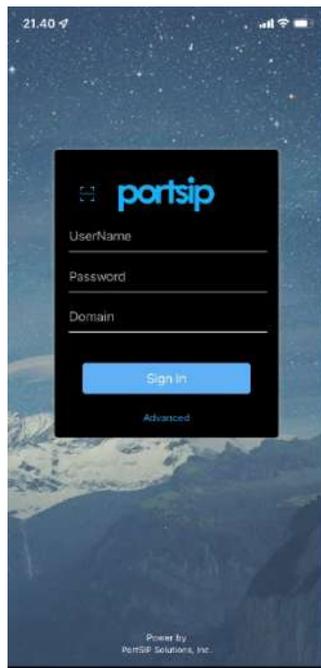


Gambar 21 Route VPN

Pada informasi tersebut menampilkan gateway server dengan gateway 103.242.124.10. pada segi komputer klien yang ditumpangi oleh komputer server dari kantor cabang tersebut saling terhubung dengan komputer klien pada kantor cabang lainnya. Ini membuktikan bahwa dengan adanya VPN PPTP (Point to point tunnelling) maka jaringan yang ada bersifat private dan tanpa melewati internet.

6. PortSIP

PortSIP UC merupakan aplikasi softphone berbasis SIP yang dapat digunakan untuk melakukan panggilan suara ataupun video. Aplikasi ini dapat ditemukan pada platform pusat unduhan yang disediakan ios maupun android. Dan dalam penggunaannya aplikasi dapat digunakan secara gratis ketika melakukan panggilan suara. Berikut untuk tampilan dari aplikasi PortSIP UC.

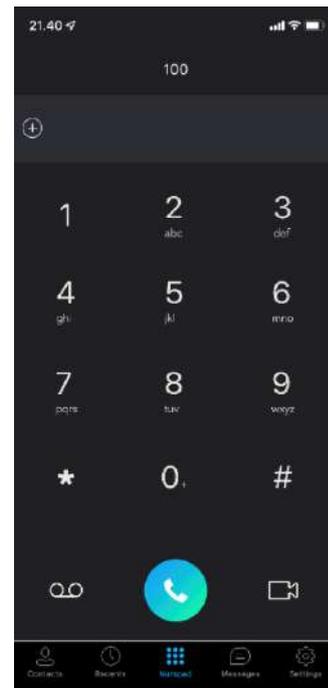


Gambar 22 Halaman Login PortISP

Keterangan:

- Username, digunakan untuk id pengguna yang telah didaftarkan pada asterisk pada server linux.
- Password, Kata sandi pada pengguna yang telah dibuat pada asterisk.
- Domain, Alamat IP asterisk yang sedang berjalan dengan kata lain domain merupakan alamat pusat dari server asterisk yang sedang berjalan.
- Sign In, Tombol untuk masuk menuju ke user yang telah didaftarkan dengan username.
- Advanced, Pengaturan login tambahan pada aplikasi PortSIP

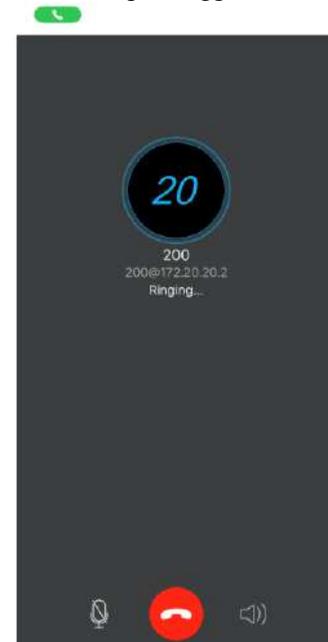
Untuk melakukan panggilan pada portsip pengguna diharuskan untuk masuk terlebih dahulu dengan username dan password yang telah didaftarkan sebelum nya selain itu domain alamat dari server asterisk juga harus terhubung. Jika username ataupun domain tidak valid maka pengguna tidak dapat masuk ke asterisk dan tidak dapat melakukan panggilan. Berikut merupakan gambar aplikasi portsip pada halaman beranda ketika siap melakukan panggilan.



Gambar 23 Halaman Utama PortISP

Setelah berhasil masuk terlihat portsip siap digunakan dengan cara menuliskan username pengguna lain pada angka pada aplikasi tersebut.

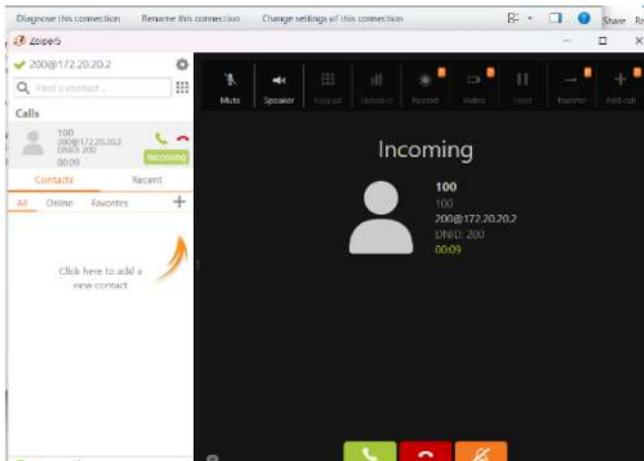
Ketika username pada pengguna lain aktif maka pemanggil dapat melakukan panggilan. Berikut merupakan gambar tampilan dari sisi pemanggil.



Gambar 24 Halaman Panggilan

Pada aplikasi Portip terdapat fitur yang dapat menunjukkan pemanggil bahwa panggilan telah berhasil dan

terhubung kepada username yang telah dituju. Hal ini ditunjukkan pada status panggilan yang bertuliskan ringing (Berdering) pada username tujuan. Berikut merupakan tampilan panggilan dari sisi penerima.



Gambar 25 Tampilan Zoiper Menerima Panggilan

Pada tampilan tersebut merupakan tampilan dari aplikasi Zoiper. Ini digunakan sebagai pembuktian terhadap asterisk yang berjalan normal sehingga menggunakan aplikasi SIP apapun akan dapat digunakan dengan kata lain aplikasi tersebut harus sudah terhubung ke server asterisk menggunakan domain yang terdapat pada server asterisk. Pada tampilan penerima panggilan terdapat tiga aksi yang dapat dilakukan oleh penerima yaitu menerima panggilan, menolak panggilan dan mengabaikan panggilan. Pada tampilan tersebut juga dapat dilihat bahwa username pemanggil juga ditampilkan.

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, penulis berhasil melakukan perancangan VoIP menggunakan VPN Gateway-to-Gateway, dengan demikian ada beberapa kesimpulan yang dapat diambil dari penelitian ini, antara lain:

1. Sistem VoIP dapat dibangun oleh perusahaan itu sendiri dikarenakan konfigurasi yang dilakukan cukup mudah namun perlu di waspadai terhadap resiko keamanannya, maka dari itu agar system VoIP tersebut aman dari serangan keamanan yang ada, dibangunlah topologi jaringan yang di topangi VPN Gateway-To-Gateway sebagai media transmisi data dari system VoIP tersebut, VPN ini menggunakan protokol PPTP (Point To Point Tunneling). Dari data keamanan yang telah di teliti sebelum nya menunjukkan bahwa dengan menggunakan VPN Gateway-To-Gateway sistem VoIP tidak terbaca oleh pihak ketiga / Penyedia Jaringan Internet, karena VPN ini telah mendukung enkripsi data.
2. Dibandingkan dengan penggunaan penyedia jasa VoIP pihak ketiga tentu penggunaan VoIP pada penelitian ini lebih murah, serta tidak memerlukan biaya berlangganan

bulanan. Dengan perawatan yang cukup mudah serta perbaikan yang mampu di kelolah oleh perusahaan itu sendiri.

V. SARAN

Peneliti menyadari bahwa dalam penelitian ini masih ditemukan kekurangan yang perlu diperbaiki oleh peneliti berikutnya. Penelitian ini hanya bersifat perancangan suatu sistem panggilan suara melalui jaringan internet, namun seolah olah menggunakan jaringan lokal. Penelitian ini juga belum menunjukkan data yang menjamin tingkat keamanannya. Maka dari itu ada beberapa saran dari penulis yang dapat digunakan untuk peneliti berikutnya, antara lain:

1. Penelitian ini hanya melakukan perancangan sistem VoIP menggunakan VPN PPTP yang artinya penelitian ini tidak menguji tingkat keamanan berdasarkan data. Melainkan hanya berdasarkan tingkat keamanan VPN yang sudah diteliti oleh peneliti sebelumnya. Diharapkan peneliti berikutnya mampu memberikan data yang menunjukkan bagaimana tingkat keamanan VoIP menggunakan VPN PPTP.
2. Pada penelitian ini tidak melakukan pengujian pada segi *latency* / keterlambatan suara berdasarkan data karena penelitian ini hanya sebatas perancangan. Sehingga diharapkan peneliti berikutnya menyertakan pengujian pada segi *latency* suara dalam penggunaan sistem VoIP berbasis VPN PPTP.

REFERENSI

- [1] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 14–20, 2020.
- [2] "Teknologi VoIP Jadi Andalan Pelaku Penipuan Online." [Online]. Available: <https://www.cnnindonesia.com/nasional/20150527070805-12-55915/teknologi-voip-jadi-andalan-pelaku-penipuan-online>. [Accessed: 18-Mar-2023].
- [3] "Get Started * Asterisk." [Online]. Available: <https://www.asterisk.org/get-started/>. [Accessed: 18-Mar-2023].
- [4] P. Dulany, C. S. Kim, and J. T. Yu, "A Performance Analysis of Gateway-to-Gateway VPN on the Linux Platform," *Computer (Long Beach, Calif.)*, no. January 2006, 2014.
- [5] J. Jupriyadi, D. P. Putra, and S. Ahdan, "Analisis Keamanan Voice Over Internet Protocol (VOIP) Menggunakan PPTP dan ZRTP," *J. VOI (Voice Informatics)*, vol. 9, no. 2, 2020.