

Keamanan Jaringan VLAN dan VoIP Menggunakan *Firewall*

Irfan^{a,1*} Ramdan Satra^{a,2}, Farniwati Fattah^{a,3}

^a Program Studi Teknik Informatika, Universitas Muslim Indonesia, Jalan Urip Sumoharjo KM.05, Makassar, 90231, Indonesia

¹ irfanfanfanfan0411@gmail.com; ² ramdan@umi.ac.id; ³ farniwati.fattah@umi.ac.id

*corresponding author

INFORMASI ARTIKEL

Diterima : 05 – 02 – 2021
Direvisi : 19 – 02 – 2021
Diterbitkan : 26 – 02 – 2021

Kata Kunci:
VoIP
VLAN
Firewall

ABSTRAK

Jaringan komputer adalah suatu hal yang tidak bisa dipisahkan dengan konfigurasi dan rancangan sebuah topologi, terutama jika komputer tersebut memiliki jumlah jaringan yang sangat banyak maka diperlukan sebuah rancangan jaringan yang saling terkoneksi dan terintegrasi, sebuah komunikasi yang handal didukung oleh sebuah keamanan data yang akan mempengaruhi tingkat layanan internet atau QOS (*Quality Of Service*). Teknologi yang dipakai adalah VoIP (*Voice Over Internet Protokol*) dan VLAN (*Virtual Local Area Network*), teknologi tersebut bisa diimplementasikan di lingkungan rumah, pada kantor dengan posisi bangunan bertingkat dan berguna untuk mengganti panggilan ke luar negeri dengan menggunakan VoIP biaya dapat ditekan mungkin, dan VLAN jaringan lokal virtual, dimana dengan teknologi tersebut jumlah perangkat yang digunakan dapat diminimalisir namun dengan kinerja yang lebih optimal. Untuk keamanan dalam pembuatan teknologi tersebut yaitu firewall dimana firewall akan memblok *MAC Address* yang berusaha menyadap atau mengambil data suara secara illegal. Hasilnya dengan menggunakan firewall jalur komunikasi VLAN dan VoIP cukup aman karena firewall mampu mengoptimalkan keamanan jaringan dan membatasi hak akses berdasarkan *MAC Address* dalam sistem yang dibuat.

This is an open access article under the [CC-BY-SA](#) license.



I. Pendahuluan

Di suatu instansi atau perusahaan terdapat beberapa orang/karyawan yang menghendaki pengambilan data secara illegal ataupun perusahaan jaringan pada institusi tertentu. Untuk menghindari hal-hal yang tidak diinginkan, dilakukanlah berbagai macam cara untuk melindungi komputer atau jaringan komputer internal yang terhubung dengan internet. Maka dari itu dibutuhkan suatu penangkal yang dapat melindungi data ataupun dokumen penting, maka dikenalkanlah firewall.

Firewall sendiri mengandung pengertian sebagai “pos pemeriksa” yang mengevaluasi trafik-trafik yang keluar dan masuk diantara jaringan internet atau privat dengan jaringan luar, mengizinkan trafik-trafik tertentu dan memblok yang lainnya. Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.

Berdasarkan hasil penelitian membuat optimasi jaringan LAN menggunakan VLAN dan VoIP, tetapi dalam penelitian tersebut hanya membahas tentang pembuatan VLAN dan konfigurasi VoIP tetapi tidak ada pembuatan keamanan dalam teknologi VoIP. Maka dari itu akan dilanjutkan penelitian dengan membuat atau menambahkan keamanan dalam teknologi VoIP [1].

Berdasarkan hasil penelitian penerapan *voice over internet protocol* (VoIP) untuk optimalisasi jaringan pada badan kependudukan dan keluarga berencana nasional, dalam penelitian tersebut peneliti menggunakan *virtual privat network* (VPN) dalam penelitian tersebut. Sedangkan pada penelitian ini untuk mengamankan komunikasi VoIP menggunakan firewall [2]

Berdasarkan uraian di atas akhirnya peneliti akan melakukan penelitian dengan menambahkan keamanan dalam sebuah teknologi VoIP. Dengan ditambahkan suatu teknologi tersebut maka diharapkan dapat menangani permasalahan pengambilan data secara illegal.

II. Metode

A. Pengertian VoIP

VoIP (*voice over internet protocol*) merupakan teknologi telekomunikasi yang berbasis IP. Teknologi ini memanfaatkan jaringan komputer untuk memberikan layanan kepada pengguna [3]. Teknologi VoIP menjadi dasar dari *Next Generation Network* (NGN) maupun jaringan seluler 4G yang digunakan oleh operator telekomunikasi masa datang. Teknik VoIP diadopsi oleh rekan-rekan Amatir Radio (ORARI) untuk menggunakan internet sebagai *relay* jarak jauh. Teknik VoIP di Amatir Radio dikenal sebagai eQSO. Inti dari VoIP terdapat pada Jantung VoIP yaitu jaringan *softswitch*, yang menyimpan semua informasi tentang pelanggan. Dalam pandangan sederhana, VoIP *softswitch* pada dasarnya memiliki tabel pemetaan nomor telepon pelanggan dan komputer atau IP alamat pelanggan. Jika ada salah satu pelanggan yang ingin melakukan panggilan maka pelanggan tersebut meminta pada *Softswitch* untuk mengetahui alamat dan tujuan pelanggan yang lain, alamat tujuan dapat menjadi alamat IP, pada dasarnya *softswitch* tempat berkumpulnya semua nomor telepon pelanggan dan IP alamat [2].

B. Protokol-protokol penunjang VoIP

Protokol-protokol yang menunjang terjadinya komunikasi VoIP adalah:

1) TCP (*Transmission Control Protocol*)

TCP merupakan protokol yang *connection oriented* yang artinya menjaga reliabilitas hubungan komunikasi *end-to-end*. Konsep dasar cara kerja TCP adalah mengirim dan menerima segmen-segmen informasi dengan panjang data bervariasi pada suatu datagram internet, TCP menjamin reliabilitas hubungan komunikasi karena melakukan perbaikan terhadap data yang rusak hilang atau kesalahan kirim.

2) UDP (*User Datagram Protocol*)

UDP merupakan salah satu protokol utama di atas IP dan merupakan transport protocol yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas, artinya pada protokol UDP ini komunikasi akan tetap berlangsung tanpa memperdulikan koneksi antara sumber dan tujuan.

3) IP (*Internet Protocol*)

Internet Protocol adalah protokol lapisan jaringan (*network layer* dalam *OSI Reference Model*) atau protokol lapisan *internetwork* (*internetwork layer* dalam *DARPA Reference Model*) yang digunakan oleh protokol TCP/IP untuk melakukan pengalamatan dan *routing* paket data antar *host* di jaringan komputer berbasis TCP/IP.

4) H.323

H.323 adalah salah satu dari rekomendasi ITU-T (*International Telecommunications Union Telecommunications*). H.323 merupakan standar yang menentukan komponen, protokol, dan prosedur yang menyediakan layanan komunikasi multimedia, layanan tersebut adalah komunikasi audio, video, dan data *real-time*, melalui jaringan berbasis paket (*packet based network*).

5) SIP (*Session Initiation Protocol*)

SIP adalah suatu *signalling protocol* pada *layer* aplikasi yang berfungsi untuk membangun, memodifikasi, dan mengakhiri suatu sesi multimedia yang melibatkan satu atau beberapa pengguna. Sesi multimedia adalah pertukaran data antar pengguna yang bisa meliputi suara, video, dan teks, IP tidak menyediakan layanan secara langsung, tetapi menyediakan pondasi yang dapat digunakan oleh protokol aplikasi lainnya untuk memberikan layanan yang lengkap bagi pengguna, misalnya dengan RTP (*Real Time Transport Protocol*) untuk transfer data secara *real-time* [2].

C. VLAN

VLAN (*Virtual LAN*) adalah suatu model jaringan yang membagi jaringan secara logikal ke dalam beberapa VLAN yang berbeda. VLAN tidak terbatas pada kondisi fisik jaringan seperti pada LAN, VLAN dapat di konfigurasi secara virtual tanpa harus melihat kondisi peralatan [4]. Rancang bangun jaringan VLAN memanfaatkan pihak ketiga yaitu ISP (*Internet Service Provider*) sebagai penyedia internet yang merupakan layanan yang diberikan secara luas kepada pihak manapun, tanpa harus mendapatkan *account* terlebih dahulu. Dalam hal ini, internet digunakan sebagai penunjang yang sangat penting agar dapat membuat akses komunikasi dengan menggunakan jaringan LAN dan VLAN sehingga komunikasi dalam kantor yang memiliki ruangan-ruangan terpisah dapat dilakukan dengan cepat [1]. VLAN berfungsi untuk membagi *broadcast* domain yang semula lebih besar menjadi dua atau lebih *broadcast* domain yang lebih kecil. VLAN dapat dibuat berdasarkan departemen, fungsi pekerjaan, dan lain-lain tanpa terpengaruh oleh lokasi fisik *host*. VLAN dapat meningkatkan kinerja jaringan secara keseluruhan. Keuntungan *Virtual Local Area Network* (VLAN).

Beberapa tujuan utama dari implementasi VLAN pada jaringan antara lain :

- 1) *Security* implementasi VLAN dalam suatu perusahaan memungkinkan terkontrolnya keamanan data dalam tiap-tiap departemen karena berada dalam satu *broadcast* domain yang sama.

- 2) *Cost Reduction* mengurangi biaya yang akan dikeluarkan apabila terdapat penambahan jaringan dan lebih efisien dalam pemakaian *bandwidth* dan uplinks.
- 3) *Higher Performance* memisahkan jaringan layer 2 ke dalam berbagai *logical workgroup (broadcast domain)* yang dapat mengurangi *traffic* data yang tidak diperlukan dan meningkatkan *performance* jaringan.
- 4) *Broadcast Storm Mitigation* penerapan VLAN dapat mengurangi jumlah *device* yang turut serta dalam sebuah *broadcast storm*.
- 5) *Improved IT Staff Efficiency* penerapan VLAN memudahkan pengaturan jaringan dan konfigurasi VLAN dapat langsung tersebar apabila ada sebuah *switch* baru yang terhubung ke dalam jaringan tersebut [5].

D. Firewall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware, software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Segmen tersebut dapat merupakan sebuah *workstation, server, router*, atau *local area network (LAN)* anda. Konfigurasi sederhananya: pc (jaringan local) $\leftarrow\equiv\rightarrow$ *firewall* $\leftarrow\equiv\rightarrow$ internet (jaringan lain). Langkah-langkah membangun firewall yaitu :

- 1) Mengidentifikasi bentuk jaringan yang dimiliki khususnya topologi yang digunakan serta *protocol* jaringan, akan memudahkan dalam mendesain sebuah *firewall*.
- 2) Menentukan *Policy* atau kebijakan. Penentuan kebijakan atau *Policy* merupakan hal yang harus dilakukan, baik atau buruknya sebuah *firewall* yang di bangun sangat ditentukan oleh *policy/kebijakan* yang diterapkan. Diantaranya [6] :
 - a. Menentukan apa saja yang perlu dilayani. Artinya, apa saja yang akan dikenai *policy* atau kebijakan yang akan kita buat.
 - b. Menentukan individu atau kelompok- kelompok yang akan dikenakan *policy* atau kebijakan tersebut.
 - c. Menentukan layanan-layanan yang dibutuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
 - d. Berdasarkan setiap layanan yang digunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
 - e. Menerapkan semua *policy* atau kebijakan tersebut.
- 3) Menyiapkan *Software* atau *Hardware* yang akan digunakan baik itu *operating system* yang mendukung atau *software-software* khusus pendukung *firewall* seperti *ipchains*, atau *iptables* pada linux, dan sebagainya. Serta konfigurasi *hardware* yang akan mendukung *firewall* tersebut.
- 4) Melakukan tes konfigurasi. Pengujian terhadap *firewall* yang telah selesai dibangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool yang biasa dilakukan untuk mengaudit seperti *nmap*.

Cara-cara firewall dalam melindungi jaringan komputer internal, antara lain:

- a) Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujuan yang tidak diinginkan.
- b) Menolak dan menyaring paket data yang berasal dari jaringan internal ke internet. Contohnya ketika ada pengguna jaringan internet akan mengakses situs-situs porno.
- c) Menolak dan menyaring paket data berdasarkan konten yang tidak diinginkan. Misalnya *firewall* yang terintegrasi pada suatu antivirus akan menyaring dan mencegah file yang sudah terjangkit virus yang mencoba memasuki jaringan internal.

Melaporkan semua aktivitas jaringan dan kegiatan firewall.

E. Pengertian dan Konsep Keamanan Jaringan

Keamanan jaringan atau (*Network Security*) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer. *Network security* melibatkan otorisasi akses ke data dalam jaringan yang dikendalikan oleh administrator jaringan. Pengguna (*user*) memilih atau diberi ID dan *password* atau informasi otentikasi lain yang memungkinkan mereka untuk mengakses informasi dan program dalam wewenang mereka sendiri. *Network security* terlibat dalam organisasi, perusahaan, dan jenis lembaga lainnya. Seperti bagaimana mengamankan jaringan, serta melindungi dan mengawasi operasi yang dilakukan. Dimana cara paling umum dan sederhana untuk melindungi sumber daya jaringan (*network resource*) adalah dengan menetapkan nama yang unik dan *password* yang sesuai.

Konsep keamanan jaringan :

- 1) *Confidentiality* (kerahasiaan)

Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

2) *Integrity* (integritas)

Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

3) *Availability* (ketersediaan)

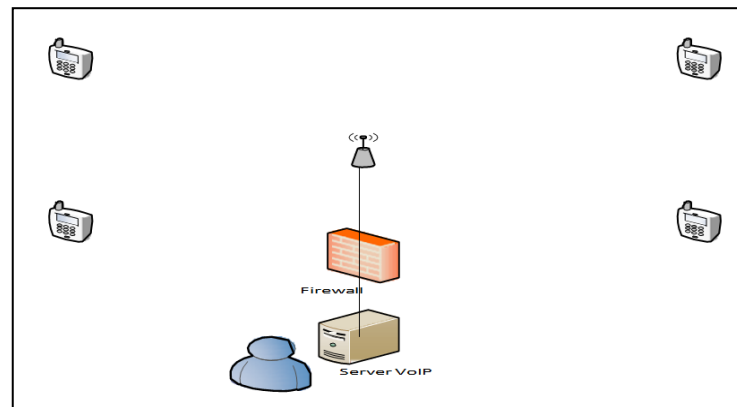
Ketersediaan adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

III. Hasil dan Pembahasan

A. Perancangan Sistem

Dalam pengerjaan tugas akhir ini penulis menggunakan tiga kondisi sistem yaitu sistem tersebut VoIP (*Voice Over Internet Protokol*), VLAN (*Virtual Area Network*), dan *firewall*. Berikut tiga gambaran umum sistem, yang akan digunakan untuk pengerjaan tugas akhir ini

1) Rancangan Topologi



Gambar 1. Rancangan Topologi

2) Pembuatan VoIP

Setelah membuat topologi akan dilakukan konfigurasi VoIP menggunakan *asterisk*. Setelah menginstall *asterisk* maka Konfigurasi VoIP akan di buat pertama pada file *sip.conf*

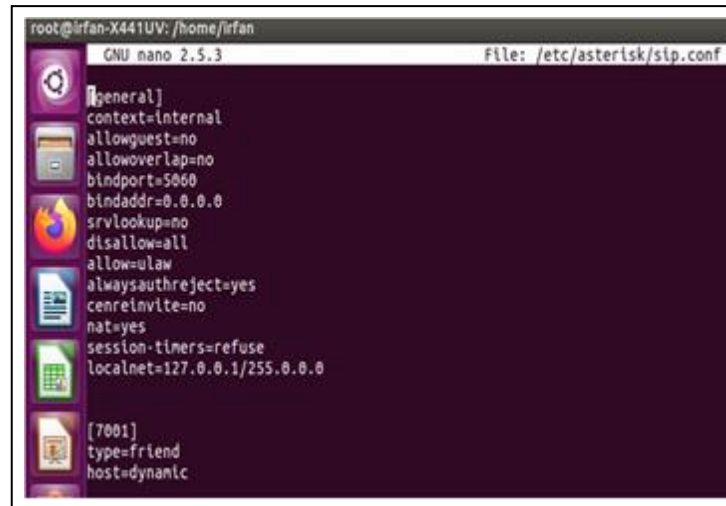
```

Asterisk cleanly ending (0).
Executing last minute cleanups
root@irfan-X441UV:/home/irfan# mv /etc/asterisk/sip.conf /etc/asterisk/sip.conf.orig
mv: target 'orig' is not a directory
root@irfan-X441UV:/home/irfan# mv /etc/asterisk/sip.conf /etc/asterisk/sip.conf.orig
root@irfan-X441UV:/home/irfan# vi /etc/asterisk/sip.conf
root@irfan-X441UV:/home/irfan# nano /etc/asterisk/sip.conf

```

Gambar 2. Konfigurasi sip.conf

Setelah itu masukkan perintah pada file *sip.conf* dimana perintahnya yaitu untuk membuat panggilan antar *client*, *username*, *password*, *port* dan *localnet*, terlihat pada gambar 3 dan 4



```

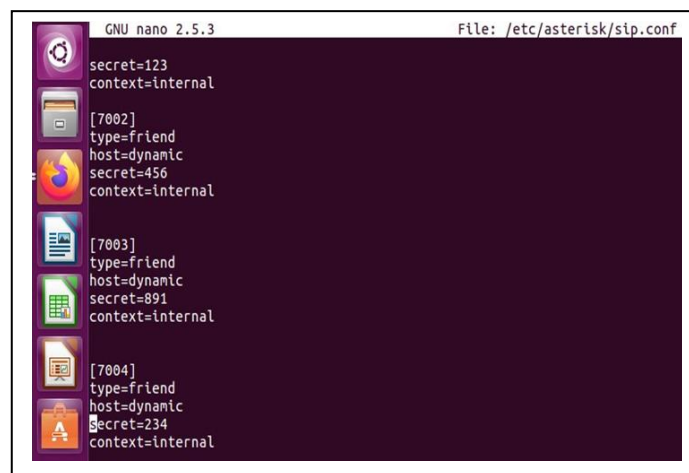
root@irfan-X441UV: /home/irfan
GNU nano 2.5.3 File: /etc/asterisk/sip.conf

[general]
context=internal
allowguest=no
allowoverlap=no
bindport=5060
bindaddr=0.0.0.0
srlookup=no
disallow=all
allow=ulaw
alwaysauthreject=yes
cenreinvite=no
nat=yes
session-timers=refuse
localnet=127.0.0.1/255.0.0.0

[7001]
type=friend
host=dynamic

```

Gambar 3. Isi konfigurasi file sip.conf



```

GNU nano 2.5.3 File: /etc/asterisk/sip.conf

secret=123
context=internal

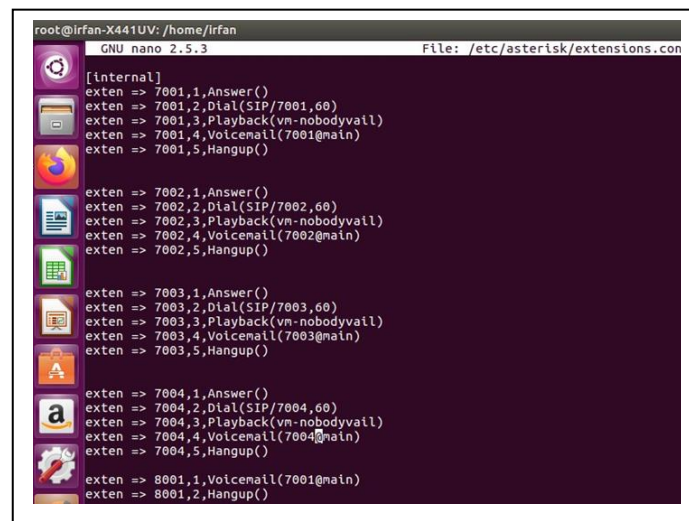
[7002]
type=friend
host=dynamic
secret=456
context=internal

[7003]
type=friend
host=dynamic
secret=891
context=internal

[7004]
type=friend
host=dynamic
secret=234
context=internal

```

Gambar 4. Lanjutan gambar 3



```

root@irfan-X441UV: /home/irfan
GNU nano 2.5.3 File: /etc/asterisk/extensions.conf

[internal]
exten => 7001,1,Answer()
exten => 7001,2,Dial(SIP/7001,60)
exten => 7001,3,Playback(vn-nobodyvail)
exten => 7001,4,Voicemail(7001@main)
exten => 7001,5,Hangup()

exten => 7002,1,Answer()
exten => 7002,2,Dial(SIP/7002,60)
exten => 7002,3,Playback(vn-nobodyvail)
exten => 7002,4,Voicemail(7002@main)
exten => 7002,5,Hangup()

exten => 7003,1,Answer()
exten => 7003,2,Dial(SIP/7003,60)
exten => 7003,3,Playback(vn-nobodyvail)
exten => 7003,4,Voicemail(7003@main)
exten => 7003,5,Hangup()

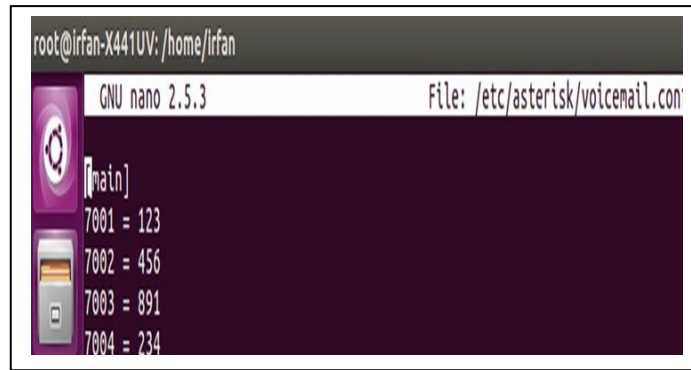
exten => 7004,1,Answer()
exten => 7004,2,Dial(SIP/7004,60)
exten => 7004,3,Playback(vn-nobodyvail)
exten => 7004,4,Voicemail(7004@main)
exten => 7004,5,Hangup()

exten => 8001,1,Voicemail(7001@main)
exten => 8001,2,Hangup()

```

Gambar 5. Isi file extensions.conf

Setelah itu masukkan perintah pada file sip.extensions dimana perintahnya yaitu untuk mengatur panggilan dalam VoIP seperti menerima, melakukan panggilan yang dituju, pemutaran pada saat melakukan panggilan, mengirim pesan suara dan menutup panggilan terlihat pada gambar di atas.



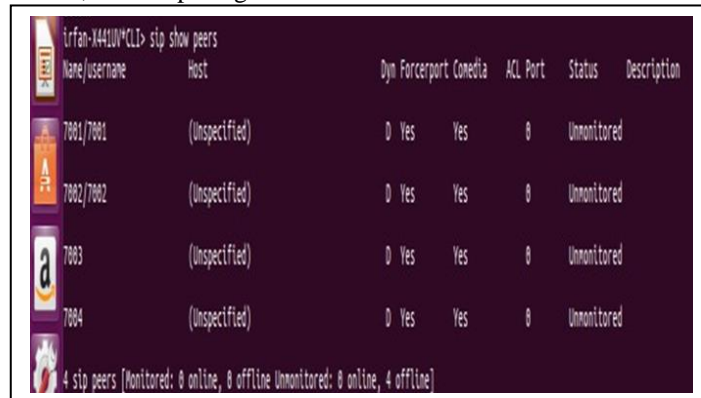
```

root@Irfan-X441UV: /home/Irfan
GNU nano 2.5.3 File: /etc/asterisk/voicemail.conf
[main]
7001 = 123
7002 = 456
7003 = 891
7004 = 234

```

Gambar 6. Isi file *voicemail.conf*

Setelah itu masukkan perintah pada file *sip.voicemail* dimana perintahnya yaitu untuk mengeksekusi *username* dan *password*, terlihat pada gambar di atas.



```

Irfan-X441UV*CLI> sip show peers
Name/Username      Host                Dyn Forceport Conedia ACL Port Status Description
-----
7001/7001          (Unspecified)      D Yes Yes      0 Unmonitored
7002/7002          (Unspecified)      D Yes Yes      0 Unmonitored
7003               (Unspecified)      D Yes Yes      0 Unmonitored
7004               (Unspecified)      D Yes Yes      0 Unmonitored
4 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 4 offline]

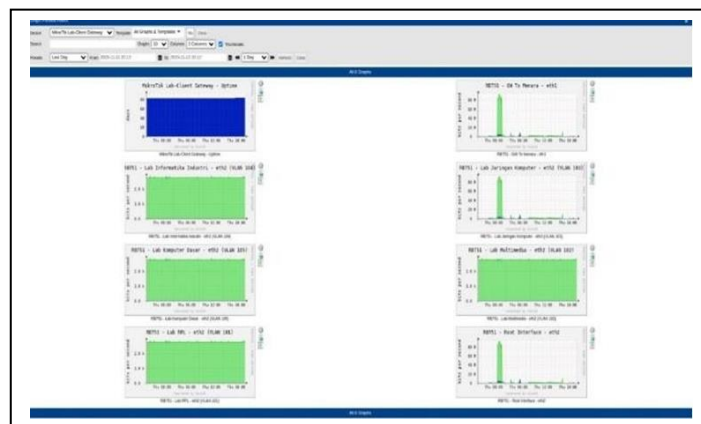
```

Gambar 7. *User* telah terdaftar

Pada gambar di atas menandakan bahwa *user* yang telah dibuat saat ini telah terdaftar.

4) VLAN

Selanjutnya untuk pembuatan VLAN peneliti memanfaatkan VLAN yang ada pada lokasi penelitian terlihat pada gambar dibawah ini.



Gambar 8. VLAN

5) Firewall

Untuk *firewall* sama seperti VLAN yaitu memanfaatkan *firewall* yang ada di lokasi penelitian, terlihat pada gambar dibawah ini.

NAME	MANUFACTURER	MAC	FIXED IP	USER GUEST	DOWN	UP	FIRST SEEN	LAST SEEN
192.168.1.101	Huawei	0800-2000-1001	-	User	00	00	04/04/2021 11:00:00	10/10/2021 11:00:00
192.168.1.102	Huawei	0800-2000-1002	-	User	00	00	08/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.103	Huawei	0800-2000-1003	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.104	Huawei	0800-2000-1004	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.105	Huawei	0800-2000-1005	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.106	Huawei	0800-2000-1006	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.107	Huawei	0800-2000-1007	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.108	Huawei	0800-2000-1008	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.109	Huawei	0800-2000-1009	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.110	Huawei	0800-2000-1010	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.111	Huawei	0800-2000-1011	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.112	Huawei	0800-2000-1012	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.113	Huawei	0800-2000-1013	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.114	Huawei	0800-2000-1014	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.115	Huawei	0800-2000-1015	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.116	Huawei	0800-2000-1016	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.117	Huawei	0800-2000-1017	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.118	Huawei	0800-2000-1018	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.119	Huawei	0800-2000-1019	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00
192.168.1.120	Huawei	0800-2000-1020	-	User	00	00	01/10/2021 11:00:00	10/10/2021 11:00:00

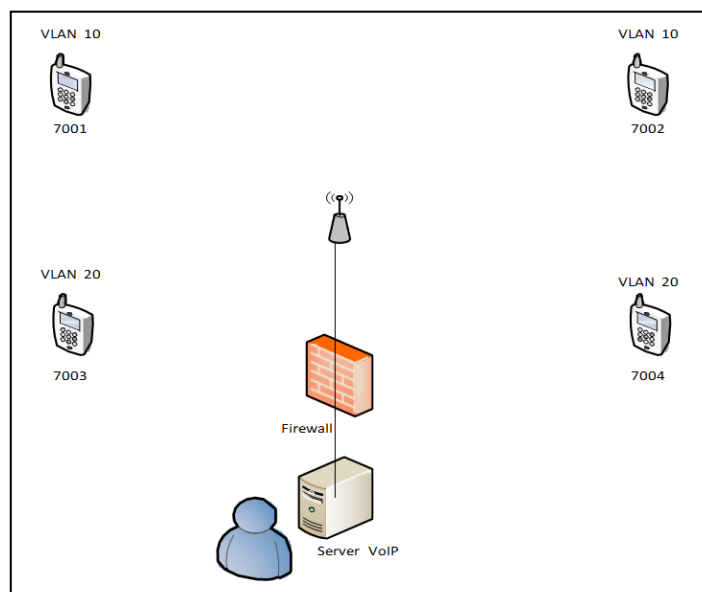
Gambar 9. Daftar MAC Address yang terkoneksi

Pada gambar diatas terlihat semua user yang masuk dalam jaringan server disini akan digunakan firewall filter MAC address untuk memblock user yang akan menyadap atau mengambil data suara.

6) Implementasi

a) Implementasi Topologi

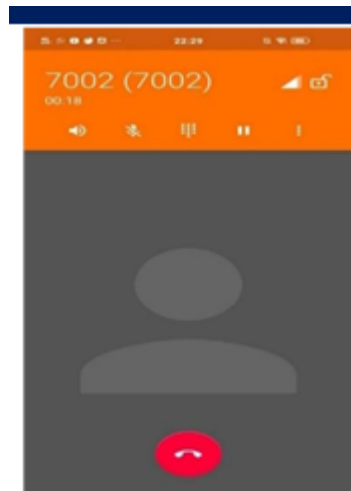
Topologi yang digunakan yaitu topologi star menggunakan Access Point sebagai node tengah untuk saling terhubung satu sama lain dari client server menuju ke server atau sebaliknya. Terdapat 4 client atau user yang masing-masing memiliki username 7001, 7002, 7003, dan 7004. 7001 dan 7002 adalah VLAN 10 dan 7003 dan 7004 adalah VLAN 20, ditunjukkan pada gambar dibawah ini.



Gambar 10. Topologi

b) Implementasi VoIP

Setelah konfigurasi yang dilakukan untuk membuat jalur komunikasi VoIP dengan menggunakan asterisk client bisa berkomunikasi satu sama lain. Berikut gambar komunikasi antar client

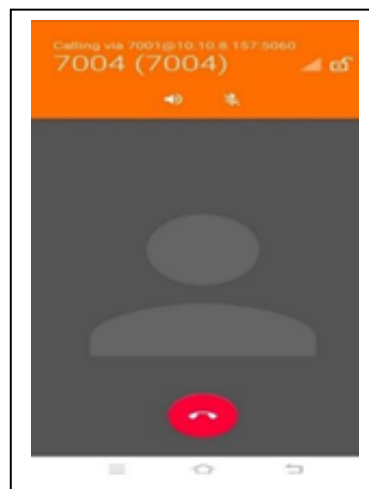


Gambar.11 Panggilan 7001 ke 7002

Pada gambar di atas ini *client* 7001 berhasil melakukan panggilan ke *client* 7002.

c) Implementasi VLAN

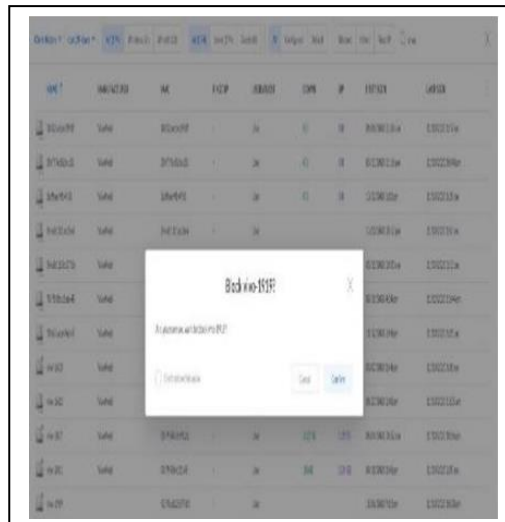
Pada gambar di bawah ini terlihat *client* 7001 tidak bisa melakukan komunikasi dengan *client* 7004 di karenakan *client* 7001 dan *client* 7004 berbeda VLAN dimana *client* 7001 berada pada VLAN 10 dan *client* 7004 berada pada VLAN 20



Gambar 12. VLAN

a) Implementasi Firewall

Pada gambar dibawah peneliti akan memblok *MAC address client* 7001 menggunakan *firewall filter MAC address*



Gambar 13. Firewall

Pemblokiran berhasil.

IV. Kesimpulan dan saran

Berdasarkan hasil implementasi Keamanan Jaringan VLAN dan VoIP menggunakan *firewall* dapat disimpulkan bahwa Panggilan suara pada VoIP berhasil mengirimkan suara antara *user* dalam VLAN berbeda terlihat pada hasil pengujian VLAN suara antar *client* berhasil terdengar, *client* dapat terhubung dan melakukan komunikasi sesama VLAN. Berdasarkan hasil pengujian *firewall* terlihat sistem mampu memblokir pengguna yang tidak terdaftar dalam *router*. Hal ini diharapkan dapat membantu dalam mengamankan jalur komunikasi antar *user*.

Berdasarkan kesimpulan diatas, maka penulis dapat memberikan saran-saran yang kiranya dapat melakukan pengembangan-pengembangan sistem yang lebih baik yaitu penelitian ini dapat jadi rujukan untuk penelitian selanjutnya dimana dikembangkan dengan cara menambah keamanan pada sistem tersebut berupa IDS, IPS dan lain sebagainya. Sistem yang dikembangkan dapat mencakup area MAN (*Metropolitan Area Network*) atau WAN (*Wide Area Network*).

Daftar Pustaka

- [1] A. P. Wahyu, "Optimasi Jaringan Local Area Network Menggunakan VLAN dan VOIP," *J. Inform. Pengemb. IT*, vol. 2, no. 1, pp. 54–57, 2017
- [2] Azhar and M. Badrul, "ISSN 2597-9922 | Penerapan Voice Over Internet Protokol Untuk Optimalisasi Jaringan Pada Badan Kependudukan dan Keluarga Berencana Nasional," *Prosisko*, vol. V, no. I, pp. 1–17, 2018.
- [3] H. M. Abdullah, "Perancangan Jaringan Voice Over IP (VoIP) Berbasis Raspberry Pi Untuk Sistem Komunikasi Area Remote," *TELKA - Telekomun. Elektron. Komputasi dan Kontrol*, vol. 2, no. 1, pp. 36–43, 2016.
- [4] B. B. Yoga and M. A. Raharja, "Implementasi Vlan (Virtual Local Area Network) Pada Rumah Sakit Mata Ramata," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 7, no. 3, p. 177, 2019.
- [5] T. I. Bayu and N. Nurhanif, "Model Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue," *Indones. J. Comput. Model.*, vol. 1, no. 2, pp. 55–60, 2018.
- [6] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. -Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018