Buletin Sistem Informasi dan Teknologi Islam
Vol 1, No 1, Januari, pp.xx-xx
ISSN: XXXX-XXXX

Keamanan Jaringan VLAN dan VOIP Menggunakan Firewall

Irfan

[1,2,3] *Fakultas Ilmu Kompter, Universitas Muslim Indonesia Makassar*
[1,2,3]*Jl. Urip Sumoharjo Km.5 Propinsi Sulawesi Selatan*

E-mail: irfanfanfanfan0411@gmail.com

INFORMASI ARTIKEL

Diterima : xx – xx – 20xx
Direvisi : xx – xx – 20xx
Diterbitkan : xx – xx – 20xx

Kata Kunci:
VoIP, VLAN, Firewall

ABSTRAK

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 Lokal Area Network*), teknologi tersebut bisa diimplementasikan dilingkungan 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 memblock *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.

1. Pendahuluan

Di suatu instansi atau perusahaan terdapat beberapa orang/karyawan yang menghendaki pengambilan data secara illegal ataupun perusakan 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 penangkalan yang dapat melindungi data ataupun dokumen penting, maka dikenalkanlah firewall.

Firewall sendiri megandung 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. Menurut Muammar (2004:1) 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 lingkupnya (Kusnadi, 2018).

Pada hasil penelitian yang dilakukan oleh (Wahyu, 2017) yaitu 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.

Hasil penelitian yang dilakukan oleh (Azhar et al., 2018) yaitu penerapan *voice over internet protokol* (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.

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

2. Metode

A. Pengertian VoIP

VoIP adalah teknik untuk bertelepon di atas jaringan Internet, teknologi yang dikembangkan memungkinkan untuk membangun sentral telepon sendiri hingga pesawat teleponnya. Teknologi VoIP menjadi dasar dari *Next Generation Network* (NGN) maupun jaringan selular 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 *Softswith* 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 (Azhar et al., 2018).

B. Protokol-Protokol Penunjang VoIP

Protokol-protokol yang menunjang terjadinya komunikasi VoIP adalah (Anton & Anggraini, 2008):

a. TCP (*Transmission Control Protocol*)

TCP merupakan protokol yang *connectionoriented* 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.

b. 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.

c. IP (*Internet Protocol*)

Internet Protocol adalah protokol lapisan jaringan (*network layer* dalam OSI *Reference Model*) atau protokol lapisan internet *work* (*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.

d. 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 (*packetbased network*).

e. 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 3. Sesi *multimedia* adalah pertukaran data antar pengguna yang bisa meliputi suara, video, dan text, 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* (Azhar et al., 2018).

C. *VLAN*

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan (Sofana, 2013). 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 (Rahmat, 2015). 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 (Wahyu, 2017), (Rahmat Novrianda Dasmen, 2019). 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

ISSN: XXXX-XXXX

keseluruhan. Keuntungan *Virtual Local Area Network* (VLAN)

Menurut Hucaby (2010), beberapa tujuan utama dari implementasi VLAN pada jaringan antara lain :

a. *Security* Implementasi VLAN dalam suatu perusahaan memungkinkan terkontrolnya keamanan data dalam tiap-tiap departemen karena berada dalam satu broadcast domain yang sama.
b. *Cost Reduction* Mengurangi biaya yang akan dikeluarkan apabila terdapat penambahan jaringan dan lebih efisien dalam pemakaian bandwidth dan uplinks.
c. *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.
d. *Broadcast Storm Mitigation* Penerapan VLAN dapat mengurangi jumlah device yang turut serta dalam sebuah *broadcast storm.*
e. *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 (Bayu, T. I., & Nurhanif, N, 2018).

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 lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation*, server, router, atau *local area network* (LAN) anda. Konfigurasi sederhananya: pc (jaringan local) ←==→ firewall ←==→ internet (jaringan lain). Langkah-langkah membangun firewall menurut Muammar (2004:6-7) yaitu:

1. Mengidenftifikasi bentuk jaringan yang dimiliki Mengetahui 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:
    1. Menentukan apa saja yang perlu dilayani. Artinya, apa saja yang akan dikenai *policy* atau kebijakan yang akan kita buat.
    2. Menentukan individu atau kelompok- kelompok yang akan dikenakan policy atau kebijakan tersebut.
    3. Menentukan layanan-layanan yang di butuhkan oleh tiap tiap individu atau kelompok yang menggunakan jaringan
    4. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman
    5. Menerapkankan 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 test 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: Muammar (2004:3)

1. Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
2. Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya ketika ada pengguna jaringan internet akan mengakses situs-situs porno.
3. Menolak dan menyaring paket data berdasakan 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 (Kusnadi, 2018).

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 di rancang 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 di ubah, dan langkah-langkah harus di ambil untuk memastikan bahwa data tidak dapat di ubah oleh orang-orang yang tidak berkepentingan.
3. *Availability (ketersediaan)*

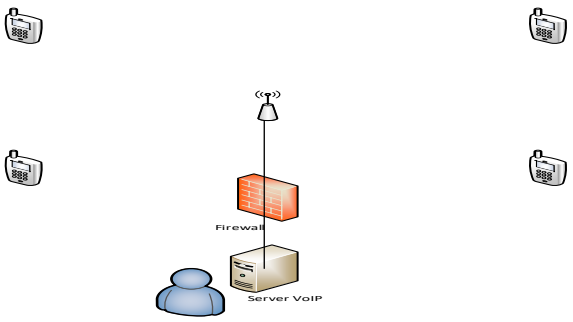
Ketersediaan adalah konsep terbaik yang dapat dipastikan dalam memelihara semua hardware, melakukan perbaikan terhadap hardware sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

3. Hasil dan Pembahasan

3.1 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

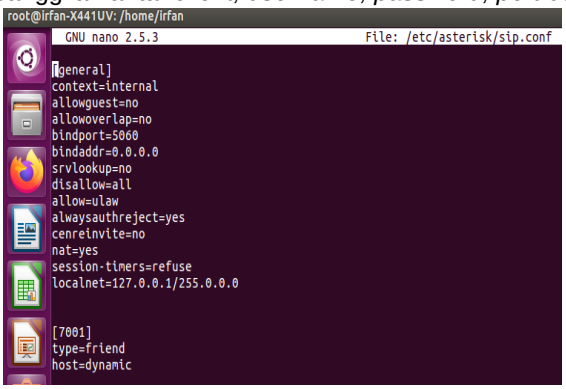
2. Pembuatan VoIP

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

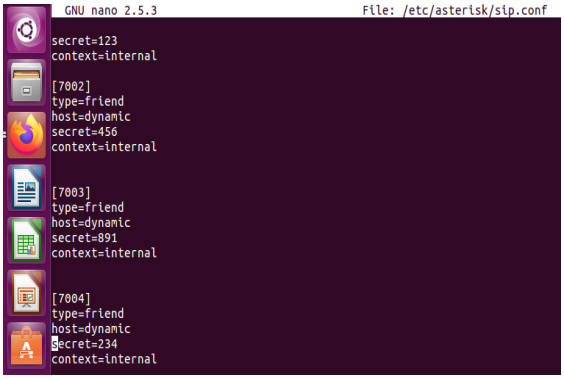
ISSN: XXXX-XXXX

Gambar 2. Konfigurasi sip.conf

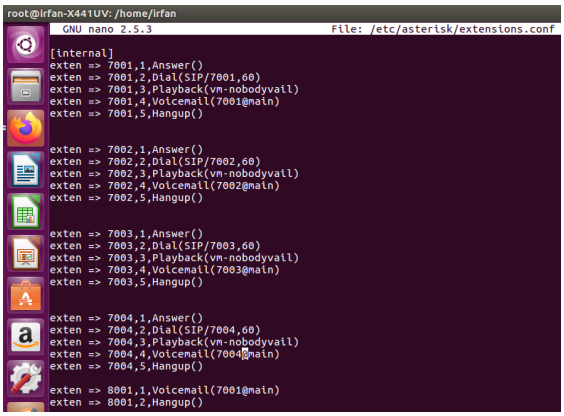
Setelah itu masukkan perintah pada file sip.conf dimana perintahnya yaitu untuk membuat panggilan antar *client, username, password, port* dan *localnet*, terlihat pada gambar 3 dan 4.



Gambar 3. isi konfigurasi file sip.conf

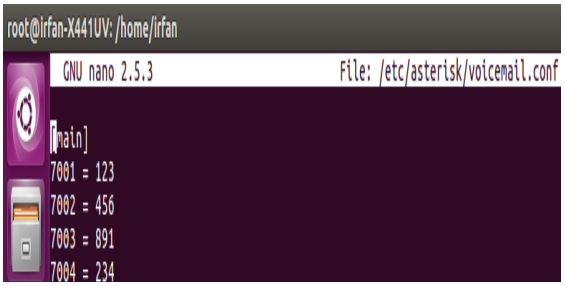


Gambar 4. Lanjutan gambar 3



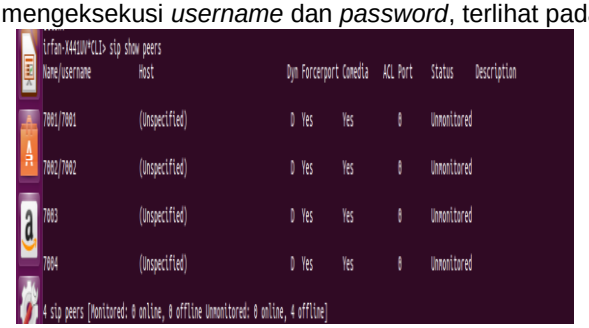
Gambar 5. Isi file extensions.conf

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



Gambar 6. Isi file voicemill.conf

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

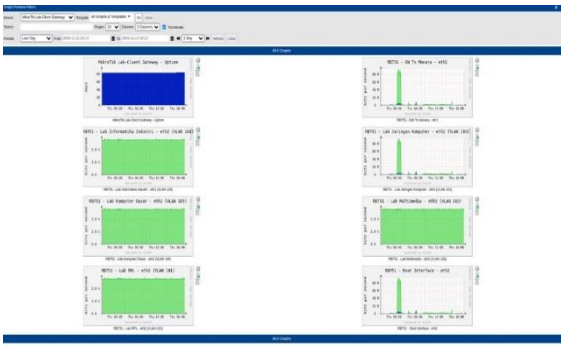


Gambar 7. *User* telah terdaftar

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

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

3. VLAN

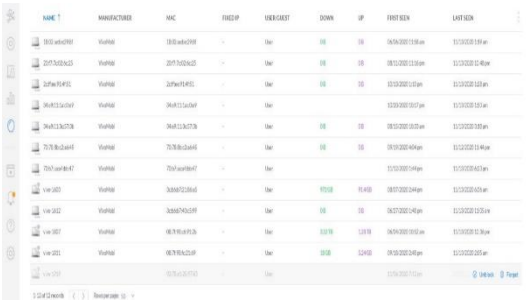


Gambar 8. VLAN

ISSN: XXXX-XXXX

4. Firewall

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



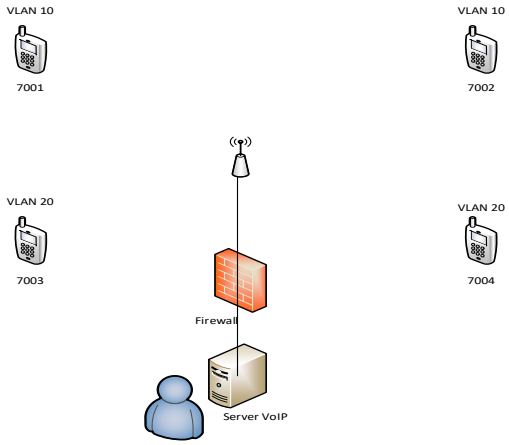
Gambar 9. Daftar MAC Address yang terkonek

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.

5. Implementasis

a. Implementasi Topologi

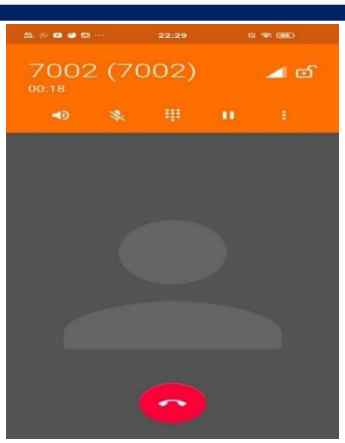
Topologi yang digunakan yaitu topologi star menggunakan *Access Point* sebagai node tengah untuk saling terhubung satu sama lain dari client server menuju ke server atau sebaliknya. Terdapat 4 client atau user yang masing-masing memiliki *username* 7001, 7002, 7003, dan 7004. 7001 dan 7002 adalah VLAN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

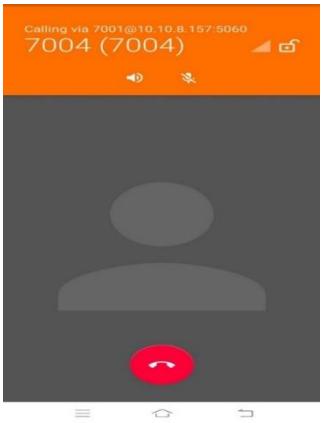


Gambar 11. Panggilan 7001 ke 7002

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

c. Implementasi VLAN

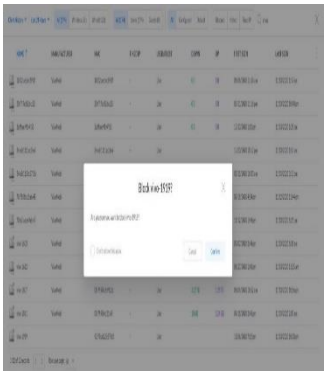
Pada gambar di bawah ini terlihat *client* 7001 tidak bisa melakukan komunikasi dengan *client* 7004 di karenakan *client* 7001 dan *client 7004* berbeda VLAN dimana *client* 7001 berada pada VLAN 10 dan *client* 7004 berada pada VLAN 20.



Gambar 12. VLAN

d. Implementasi Firewall

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



Gambar 13.Firewall

Pemblokiran berhasil.

ISSN: XXXX-XXXX

4. Kesimpulan dan Saran

4.1 Kesimpulan

Berdasarkan hasil implementasi Keamanan Jaringan VLAN dan VoIP menggunakan *firewall* dapat disimpulkan bahwa :

1. 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.

2. 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*.

4.2 Saran

Berdasarakan kesimpulan diatas, maka penulis dapat memberikan saran-saran yang kiranya dapat melakukan pengembangan-pengembangan sistem yang lebih baik yaitu :

1. Penelitian ini dapat jadi rujukan untuk penelitian selanjutnya dimana dikembangkan dengan cara menambah keamanan pada sistem tersebut berupa IDS, IPS dan lain sebagainya.

2. Sistem yang dikembangkan dapat mencakup area MAN (*Metropolitan Area Network*) atau WAN (*Wide Area Network*).

.

Daftar Pustaka

Abdullah, H. M. (2016). Perancangan Jaringan Voice Over IP (VoIP) Berbasis Raspberry Pi Untuk Sistem Komunikasi Area Remote. *TELKA - Telekomunikasi, Elektronika, Komputasi Dan Kontrol*, *2*(1), 36–43. https://doi.org/10.15575/telka.v2n1.36-43

Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (2018). *Optimalisasi Jaringan Menggunakan Firewall*. *2*(3), 17–23.

Ayuningtyas, A., Sudaryanto, S., & Cessara, D. D. (2020). Sistem Manajemen Virtual Local Area Network (VLAN) Pada Cisco Catalyst 3750 Berbasis Web. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *11*(1), 297–306. https://doi.org/10.24176/simet.v11i1.4084

Azhar, A., Badrul, M., & Akmaludin. (2018). Penerapan Voice Over Protocol (VoIP) untuk Optimalisasi Jaringan pada Badan Kependudukan dan Keluarga Berencana Nasional. *Prosisko*, *5*(1), 1–17.

Bayu, T. I., & Nurhanif, N. (2018). Model Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue. *Indonesian Journal of Computing and Modeling*, *1*(2), 55–60. https://doi.org/10.24246/j.icm.2018.v1.i2.p55-60

Wahyu, A. P. (2017). Optimasi Jaringan Local Area Network Menggunakan VLAN dan VOIP. *Jurnal Informatika:Jurnal Pengembangan IT*, *2*(1), 54–57.

Yoga, I. W. B. B., & Raharja, M. A. (2019). Implementasi VLAN (Virtual Local Area Network) pada Rumah Sakit Mata Ramata. *Jurnal Elektronik Ilmu Komputer Udayana*, *2*(7), 177–186.