Jurnal INSAN (Journal of Information Systems Management Innovation)
Volume 3 No. 1 Juni 2023
E-ISSN: 2777-1385

Perancangan Sistem Keamanan VoIP Server *Randomize number* PT Mulia Persada Indonesia Menggunakan VPN L2TP

Agra Syahputra[1], Fintri Indriyani[2], Tommi Alfian Armawan Sandi[3]

[1,2] Teknologi Informasi, Universitas Bina Sarana Informatika
[3]Teknologi Komputer, Universitas Bina Sarana Informatika
Jl. Kramat Raya No 98 - Jakarta 10450, Indonesia
e-mail: [1]putrailham160400@gmail.com, [2]fintri.fni@bsi.ac.id, [3]tommi.taf@bsi.ac.id

Abstrak - PT Mulia Persada Indonesia merupakan perusahaan yang bergerak pada layanan dan produk dalam jasa telekomunikasi, salah satunya bergerak pada bidang penjualan perangkat telepon berupa *IPPhone*. Oleh karena itu dibutuhkan sistem komunikasi yang canggih guna memenuhi kebutuhan telekomunikasi dan efisiensi nomor telepon bagi *agent telesales* di PT Mulia Persada Indonesia adalah dengan menerapkan fitur *Randomize number* (sebuah layananan nomor acak) dengan sistem VoIP server berbasis *cloudvoice* yang terhubung melalui internet untuk mengakses server sehingga dalam pengelolaan dan pemeliharaan server dapat lebih efisien. Akan tetapi sistem keamanan server yang masih tergolong minim dikarenakan hanya menggunakan NAT untuk mengubah IP Lokal menjadi IP Publik yang membuat akses server masih terbuka secara umum sehingga dapat diakses secara umum yang membuat rentan terjadinya serangan dari dan pembobolan data oleh pihak luar. Untuk itu penulis merekomendasikan dan menerapkan sistem keamanan VPN L2TP guna memecahkan masalah keamanan jaringan meningkatkan sistem keamanan server yang lebih baik sehingga data server dapat lebih aman dari tindakan serangan maupun pembobolan data, dikarenakan dari hasil pengujian yang dapat mengakses server VoIP Randomize Number hanya pada perangkat komputer IT Support yang sudah terintegrasi dengan VPN L2TP.

Kata Kunci : VoIP, telekomunikasi, *Telesales*, Keamanan Jaringan, VPN L2TP

Abstracts *- PT Mulia Persada Indonesia is a company engaged in telecommunications services and products, specifically in the field of IPPhone device sales. Therefore, an advanced communication system is required to fulfill the telecommunications needs and telephone number efficiency for telesales agents at PT Mulia Persada Indonesia. This can be achieved by implementing the Randomize number feature, a service that provides random phone numbers, using a cloud-based VoIP server system connected through the internet to access the server. This setup enables more efficient server management and maintenance. However, the server security system is currently limited as it only utilizes Network Address Translation (NAT) to convert local IP addresses into public IP addresses, leaving the server accessible to the general public. This vulnerability increases the risk of attacks and data breaches from external parties. Therefore, the author recommends implementing a VPN L2TP security system to address these network security issues and enhance the server's overall security. By doing so, the server data can be better protected against potential attacks and data breaches.*

Key Words : VoIP, telecommunications, telesales, Network Security, VPN L2TP

PENDAHULUAN

VoIP adalah sebuah sistem dalam jaringan komputer yang memungkinkan komunikasi jarak dekat maupun jarak jauh dengan menggunakan pengiriman paket data. Dalam sistem ini suara dikirimkan melalui protokol internet atau IP. Dengan menggunakan teknologi VoIP pengguna dapat melakukan panggilan suara melalui jaringan internet. (Kusuma & Aditiyo N, 2020). Dalam server VoIP terdapat fitur yang Bernama *Randomize number* yang merupakan fitur dengan sistem acak nomor. Sehingga dalam satu ekstension ketika melakukan panggilan secara otomatis nomor yang keluar akan berubah secara acak dan bukan nomor yang sama. Fitur ini biasa digunakan untuk layanan telekomunikasi telesales, fungsi dari fitur ini adalah untuk efesiensi nomor telepon dan menghindari kesan spam kepada calon pelanggan ketika mencoba melakukan panggilan Kembali kepada calon pelanggan ketika menggunakan nomor yang sama seperti pada telepon analog.

Dan salah satu hal yang paling penting dalam jaringan komputer adalah keamanan. Keamanan jaringan komputer menjadi aspek krusial dalam menjaga keutuhan dan keabsahan data, serta memberikan perlindungan terhadap informasi pengguna. Upaya perlindungan tersebut bertujuan untuk mencegah serangan dan tindakan

pencurian data yang dilakukan oleh pihak eksternal yang tidak bertanggung jawab. (Arta et al., 2018). Dan pada perancangan sistem keamanan jaringan komputer server *Randomize number* PT Mulia Persada Indonesia penulis merekomendasikan menggunakan VPN L2TP dengan IPSec guna meningkatkan keamanan VoIP server *randomize* PT Mulia Persada Indonesia menjadi lebih baik.

VPN L2TP adalah pengembangan dari sistem keamanan PPTP dan L2F yang dirancang sebagai protokol dial-up berbasis vertikal. Sistem L2TP memperluas fungsionalitas sesi *dial-up* VPN menggunakan protokol *Point-to-Point Tunneling Protocol* (PPTP) melalui jaringan internet IP Publik dengan tingkat keamanan yang lebih tinggi daripada PPTP. Protokol ini menggunakan IPSec (*Internet Protocol Security*) yang berfungsi untuk mengamankan transmisi data dalam jaringan berbasis TCP/IP. IPSec menawarkan tiga layanan utama, yaitu otentikasi dan integritas data, kerahasiaan data, serta manajemen kunci. Mikrotik RouterOS merupakan salah satu platform yang mendukung konfigurasi VPN L2TP, yang memungkinkan koneksi virtual untuk menghubungkan komputer secara privat melalui jaringan publik (Wicaksana et al., 2021).

METODE PENELITIAN

Metode penelitian yang dilakukan untuk pengumpulan data adalah sebagai Berikut:

a. Observasi

Merupakan metode pengumpulan data dengan cara melakukan pengamatan Terhadap objek penelitian secara langsung yaitu kegiatan proses penelitian dan pengelolaan penelitian pada PT Mulia Persada Indonesia dan kemudian menarik kesimpulan dari seluruh kegiatan pada objek tersebut.

b. Wawancara

Merupakan metode pengumpulan data melalui tatap muka secara langsung dengan pihak-pihak tertentu yaitu *president director*, *Operation director* dan *IT Support* PT Mulia Persada Indonesia.

c. Studi Pustaka

Studi pustaka merupakan teknik sekumpulan data untuk mempelajari buku, pencarian literatur atau referensi, catatan, dan laporan yang menjadi rujukan dalam penelitian. Proses studi pustaka ini juga diperlukan untuk mengumpulkan data. Nantinya penulis mencantumkan data tersebut dalam karya ilmiah dengan menggunakan sumber data yang valid.

VoIP adalah sebuah teknologi yang memungkinkan pengiriman trafik suara, video, dan data dalam bentuk paket melalui jaringan internet menggunakan protokol IP (*Internet Protocol*). Dalam hal ini, VoIP menggabungkan internet untuk komunikasi suara, video, dan data, dengan *Public Switched Telephone Network* atau yang biasa disebut sebagai PSTN (Nanda, 2021).

Penerapan server VoIP memiliki manfaat dalam mengurangi biaya operasional dan meningkatkan efisiensi dalam layanan telekomunikasi. Dengan menggunakan PC, laptop, atau *Smartphone*, sebagai pengganti perangkat telepon atau *IPPhone* dengan menggunakan *softphone*, yang beroperasi melalui saluran internet. (Mufida & Agus Rahayu, 2018). Sehingga pekerjaan dapat dilakukan secara *mobile* serta kemudahan dalam pemeliharaan dan perawatan dikarenakan hanya perlu menggunakan jaringan internet untuk mengakses server ketika melakukan *maintenance*.

Internet merupakan sebuah media dalam jaringan komunikasi yang digunakan untuk menghubungkan berbagai jaringan komputer dengan menggunakan protokol *Transmission Control Protocol* (TCP/IP). Protokol ini berperan sebagai standar pengalamatan dan memfasilitasi pertukaran paket data antara jaringan-jaringan tersebut. Proses ini dikenal dengan istilah *Switching Communication Protocol*, di mana paket-paket data dipindahkan melalui jaringan secara efisien dan efektif. (Aldo, 2020).

Dalam internet tentunya diperlukan keamanan jaringan. Keamanan jaringan merupakan suatu sistem yang bertujuan untuk mencegah dan mengidentifikasi penggunaan yang tidak sah, termasuk tindakan mencurigakan, dalam jaringan komputer. Sistem ini dirancang untuk melindungi *hardware* dan *software* komputer dari ancaman baik secara fisik maupun logis, serta untuk mencegah tindakan pencurian dan pembobolan data yang dapat membahayakan integritas dan kerahasiaan informasi (Tahir, 2022).

VPN (*Virtual Private Network*) adalah sebuah sistem yang digunakan untuk mengakses jaringan secara pribadi dan aman. VPN bekerja dengan melakukan enkripsi data saat pertukaran paket data terjadi. Ketika terhubung melalui VPN, koneksi internet akan melalui jalur khusus yang mengarah ke server VPN, sehingga tidak menggunakan jalur utama atau jaringan publik yang umum digunakan (Zackiansyah, 2022).

VPN L2TP merupakan sebuah pengembangan sistem keamanan jaringan yang berasal dari PPTP dengan penambahan fitur L2F. Meskipun menggunakan protokol keamanan dan enkripsi yang sama dengan PPTP, L2TP menggunakan UDP port 1701 untuk pertukaran data yang memberikan tingkat keamanan yang lebih baik. L2TP

juga bekerja secara bersamaan dengan IPSec untuk meningkatkan keamanan. Dengan menggunakan L2TP, pengguna dapat terhubung ke jaringan lokal mereka dengan keamanan yang lebih baik dari mana saja melalui jaringan internet. Selain itu, L2TP juga digunakan untuk menciptakan *Virtual Private Dial Network* (VPDN), yang memungkinkan penggunaan berbagai jenis protokol di dalamnya. (Ilyas, 2021).

Dan perangkat yang digunakan dalam perancangan dan penerapan pada VPN L2TP untuk server *Randomize number* adalah Mikrotik dengan sistem operasi RouterOs. Mikrotik merupakan perangkat router yang memiliki ukuran ebih praktis dan terdiri dari komponen *processor*, RAM dan ROM serta memori. (Laksamana et al., 2023).

Dalam penelitian berjudul "Implementasi Jaringan VPN (L2TP/IPSec) Mikrotik untuk *Remote Access Sebagai Security* selama *Work From Home* (WFH) Dalam Masa Pandemi Covid-19 di PT XL Axiata", PT XL Axiata telah menerapkan kebijakan *Work From Home* (WFH) selama pandemi Covid-19. Kebijakan tersebut memungkinkan setiap karyawan untuk terhubung ke jaringan dan data perusahaan menggunakan internet dengan IP Publik. Guna mencegah penyadapan oleh pihak yang tidak bertanggung jawab, PT XL Axiata melakukan implementasi keamanan jaringan dengan menggunakan VPN L2TP sebagai solusi keamanan data pada server mereka.

Penelitian ini berfokus pada penggunaan L2TP atau IPSec untuk menghubungkan jaringan intranet perusahaan. Protokol keamanan digunakan untuk manajemen kunci dalam pertukaran data, otentikasi, dan menjaga integritas data. Implementasi ini dilakukan menggunakan perangkat *virtual* dengan bantuan *Vmware Workstation.* Pengujian dilakukan untuk memverifikasi analisis data dengan melakukan perintah ping di *command prompt* dan menggunakan *Wireshark* untuk memastikan enkripsi data paket antara jaringan yang berbeda dalam perusahaan yang sama. Dengan adanya penelitian ini, diharapkan PT XL Axiata dapat memastikan keamanan data dan integritas jaringan selama masa WFH di tengah pandemi Covid-19, sehingga para karyawan dapat terhubung dengan aman ke jaringan perusahaan dan menjalankan tugas-tugas mereka dari rumah. (Rahino & Susila, 2022).

Dalam penelitian yang berjudul "Penerapan *Firewall* dan Protokol IPSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik di PT Neu Indonesia", dilakukan upaya untuk meningkatkan keamanan jaringan komputer di dalam jaringan Wide Area Network (WAN). Sebelumnya, keamanan data dalam jaringan tersebut hanya mengandalkan *firewall* bawaan Windows, yang rentan terhadap ancaman internal maupun eksternal. Untuk mengatasi hal ini, dilakukan implementasi *firewall* pada router guna mendeteksi malware berbahaya dari berbagai situs yang dikunjungi.

Sistem keamanan *firewall* memiliki sensitivitas yang tinggi terhadap kesalahan konfigurasi dan kegagalan dalam penerapannya. Oleh karena itu, ditambahkan pula VPN dengan protokol IPSec atau L2TP. Hal ini memungkinkan kantor pusat dan cabang di Solo untuk memiliki jaringan privat yang lebih aman dan terenkripsi dengan baik. Dengan adanya VPN, data antara cabang-cabang tersebut dapat dikirimkan melalui internet secara *private*, sehingga meningkatkan keamanan dan privasi komunikasi. Dengan penerapan *firewall* yang lebih kuat dan penambahan VPN dengan protokol IPSec atau L2TP, PT Neu Indonesia berharap dapat menciptakan jaringan yang lebih aman dan terlindungi, sehingga melindungi data sensitif perusahaan dari ancaman keamanan yang ada di jaringan publik. (Ayub et al., 2021).

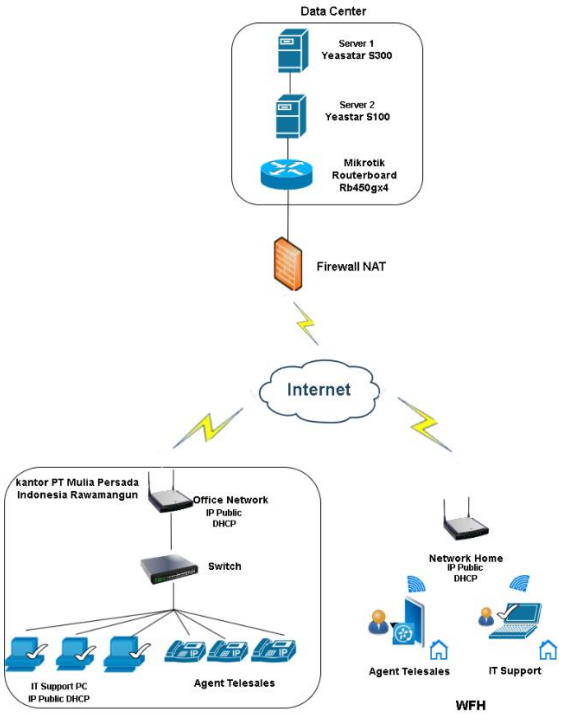
Dalam rangka memastikan keamanan dan akses yang aman ke data perusahaan, PT Datindo Infonet Prima melakukan implementasi jaringan VPN. Dengan menggunakan protokol L2TP dan IPSec, jaringan lokal perusahaan diubah menjadi jaringan publik yang terenkripsi, memungkinkan data dapat saling terkoneksi dengan aman dari perangkat yang memiliki otoritas akses VPN L2TP. Hal ini memberikan perlindungan tambahan terhadap serangan dan akses yang tidak sah ke jaringan perusahaan.

Melalui penerapan VPN, PT Datindo Infonet Prima dapat memastikan bahwa karyawan yang bekerja dari rumah dapat mengakses data dan sumber daya perusahaan dengan aman. VPN L2TP memungkinkan karyawan untuk terhubung ke jaringan perusahaan melalui perangkat komputer atau laptop yang telah dikonfigurasi dengan VPN. Dengan demikian, PT Datindo Infonet Prima dapat menjaga keamanan dan kerahasiaan data selama periode WFH, menjaga kelancaran operasional perusahaan, dan melindungi data perusahaan dari ancaman yang mungkin timbul dari jaringan publik. (Triyansa & Sobari, 2022)

HASIL DAN PEMBAHASAN

Berikut ini adalah skema jaringan yang sudah berjalan di PT Mulia Persada Indonesia dengan menggunakan *firewall* NAT.

A. Topologi Jaringan



Sumber : PT Mulia Persada Indonesia (2023)

Gambar 1. Topologi Jaringan VoIP Server dengan *Firewall* NAT PT Mulia Persada Indonesia.

Untuk jaringan yang diterapkan pada server *Randomize number* PT Mulia Persada Indonesia adalah dengan mengintegrasikan antara *cloud computing* melalui server yang ada di *data center* dengan jaringan LAN yang terdapat di kantor serta jaringan internet lainnya ketika IT *Support* sedang WFH atau sedang tidak berada dikantor sehingga server bisa diakses di manapun serta kapanpun dengan menggunakan jaringan internet untuk mempermudah *maintenance* dan pengelolaan server. Perangkat yang dimiliki PT Mulia persada Indonesia dalam penggunaan VoIP server *Randomize number* adalah sebagai berikut:

Pada *Data Center* memiliki perangka IP PBX Yeastar S300 sebagai server 1, IP PBX Yeastar S100 sebagai server 2 dan mikrotik rb450gx4 untuk *firewall* NAT. Di kantor PT Mulia Persada Indonesia memiliki perangkat *Personal computer* (PC) yang digunakan staff IT untuk *maintenance* server, *IPPhone* yang digunakan untuk *telesales* untuk melakukan panggilan telepon, Akses internet (WiFi) Indihome dan *switch* untuk menghubungkan perangkat komputer dan *IPPhone* ke internet.

Ketika WFH (*Work From Home*) atau sedang tidak berada dikantor perangkat yang dimiliki karyawan PT Mulia Persada Indonesia adalah Laptop untuk IT *Support* yang berfungsi akses internet ke server PT Mulia Persada Indonesia dan *Smartphone* bagi *agent telesales* yang sudah diinstal aplikasi *softphone* sebagai pengganti perangkat telepon *IPPhone* dikantor.

B. Arsitektur Jaringan

PT Mulia Mulia Persada Indonesia menerapkan arsitektur jaringan server dengan menggunakan *firewall* NAT (*Network Address Translation*). *Firewall* NAT merupakan protokol yang digunakan untuk mengubah alamat IP privat (IP lokal) menjadi alamat IP publik dengan cakupan global. Dengan menggunakan *firewall* NAT, sistem ini berfungsi sebagai penghubung antara IP LAN dan IP WAN, sehingga memungkinkan akses melalui internet dan memfasilitasi koneksi antara jaringan lokal dan jaringan yang lebih luas. Selain itu, *firewall* NAT juga melakukan *multiplexing* dalam arus jaringan dan mengirimkan data kembali ke internet dengan menggunakan jaringan yang lebih luas.

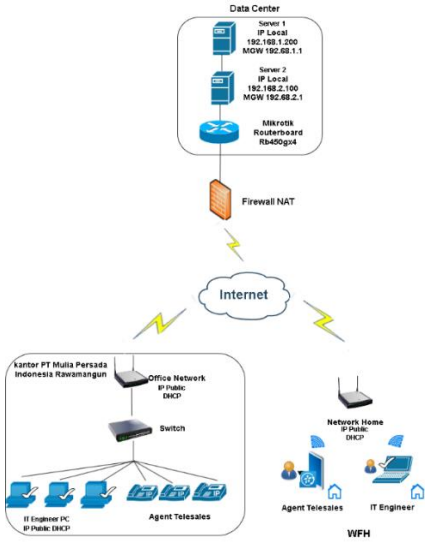
Tabel 1. IP *Address* tabel PT Mulia Persada Indonesia

No	*Details*	IP *Address*	*Gateway*	*Subnetmask*	DNS	IP *Public*	Port
1	Yeastar S300	192.168.1.200	192.168.1.1	255.255.255.0	8.8.8.8	103.53.193.150	8888
2	Yeastar S100	192.168.2.100	192.168.2.1	255.255.255.0	8.8.8.8	103.53.193.152	8888
3	Mikrotik Router Board	103.53.193.102	103.53.193.1	255.255.255.248	8.8.8.8	-	1801
4	*Personal computer*	IP DHCP	X	255.255.255.0	8.8.8.8	IP DHCP	-
5	Laptop	IP DHCP	X	255.255.255.0	8.8.8.8	IP DHCP	-

Sumber: PT Mulia Persada Indonesia (2023)

C. Skema Jaringan

Firewall NAT beroperasi dengan cara mengalihkan paket data ke *remote* internet yang terhubung dengan jaringan NAT. Ketika paket data mencapai NAT, NAT akan mencatat alamat IP tersebut dan mengubahnya menjadi nomor IP yang terkait. Selanjutnya, server akan merespons permintaan tersebut, dan alamat IP yang terlihat adalah alamat IP NAT, bukan alamat IP pengguna yang mengirim permintaan akses data. Proses ini memungkinkan server untuk menyembunyikan alamat IP asli pengguna dan mengirimkan kembali paket data dengan menggunakan alamat IP NAT ke alamat IP pengguna yang terhubung dengan server.



Sumber: PT Mulia Persada Indonesia (2023)

Gambar 2. Skema Jaringan VoIP server dengan *firewall* NAT *Randomize number* PT Mulia Persada Indonesia

D. Keamanan Jaringan

Keamanan jaringan yang diterapkan PT Mulia Persada Indonesia menggunakan *firewall* NAT *masquerade* srcnat untuk mengubah IP *Address private* menjadi IP Publik dengan konfigurasi *protocol* 17 (udp) dengan parameter (*chain*) dstnat yang mengarah ke dst *address* 103.53.193.150 port 5060 untuk diteruskan ke IP Lokal server 1 dengan alamat IP 192.168.1.200 dan *protocol* 6 (tcp) dst *address* 103.53.193.150 yang diarahkan ke IP

Lokal server 1 dengan alamat IP 192.168.1.200 dengan port 5060. udp *custom destination* port 5560 dan RTP Media parameter (*chain*) dstnat yang diarahkan ke dst *address* 103.53.193.150 *protocol* 17 (udp) ke alamat IP Lokal server 192.168.1.200 *destination* port 10000-60000 dan untuk *web* akses memakai port 8888 dan 80 untuk *protocol* 6 (tcp).

Untuk server 2 menerapkan konfigurasi *firewall* NAT dengan *protocol* 17 (udp) dengan parameter (*chain*) dstnat yang mengarah ke dst *address* 103.53.193.152 port 5060 untuk diteruskan ke IP Lokal server 1 dengan alamat IP 192.168.2.100 dan menerapkan *protocol* TLS TCP *protocol* 6 (tcp) dst *address* 103.53.193.152 yang diarahkan ke IP Lokal server 2 dengan alamat IP 192.168.2.100 dengan port 5061. RTP Media parameter (*chain*) dstnat yang diarahkan ke dst *address* 103.53.193.152 *protocol* 17 (udp) ke alamat IP Lokal server 192.168.1.200 *destination* port 10000-60000 dan untuk *web* akses memakai port 8888 dan 80 *protocol* 6 (tcp).

Untuk *mangle rule* tcp *in* dan *out* pada IP Publik server 1 dengan alamat IP Lokal 192.168.1.200 menerapkan parameter (*chain*) prerouting untuk *packet in* dan *postrouting* untuk *packet out* dengan *destination* port 8088, 8888, 8111 dan *action* yang dipilih adalah *mark connection* yang berfungsi untuk menandai suatu koneksi pada jaringan.dan untuk *mangle rule packet in* dan *out udp* menggunakan *destination port* 5060, 10000-60000.

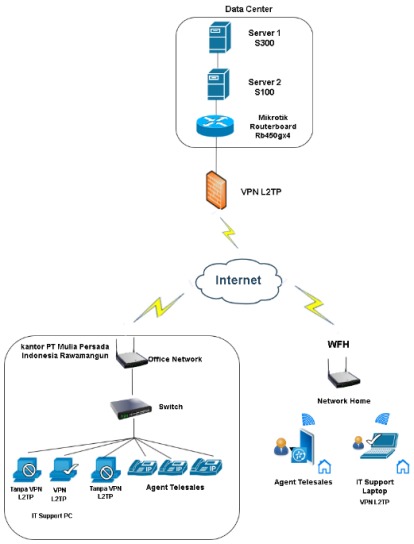
Untuk *mangle rule* tcp *in* dan *out* pada IP Publik server 2 dengan alamat IP Lokal 192.168.2.100 menerapkan parameter (*chain*) prerouting untuk *packet in* dan postrouting untuk *packet out* dengan destination port 8088, 8888, 8111 dan *action* yang dipilih adalah mark *connection* yang berfungsi untuk menandai suatu koneksi pada jaringan.dan untuk *mangle rule packet in* dan *out udp* menggunakan *destination port* 5060, 10000-60000. Untuk *service* port yang diterapkan adalah ftp dengan *ports* 21, irc dengan *ports* 6667, sip dengan *ports* 5060, 5061, 58111, 8111 dan tftp dengan *ports* 69.

E. Rancangan Jaringan Usulan

1. Jaringan Usulan

Namun lemahnya keamanan server ketika menggunakan *firewall* NAT yang membuat server dapat diakses secara bebas melalui internet yang menyebabkan rentan mengalami kebocoran data serta serangan dari pihak luar yang tidak bertanggung jawab. Penulis mengusulkan untuk melakukan perancangan VPN L2TP dengan IPSec untuk meningkatkan keamanan pada server *Randomize number* PT Mulia persada Indonesia. Untuk pengujian ini digunakan dua server yaitu IP PBX, satu buah Mikrotik Routerboard dan perangkat computer atau laptop serta jaringan internet modem (wifi).

2. Topologi Jaringan



Sumber: Penulis (2023)

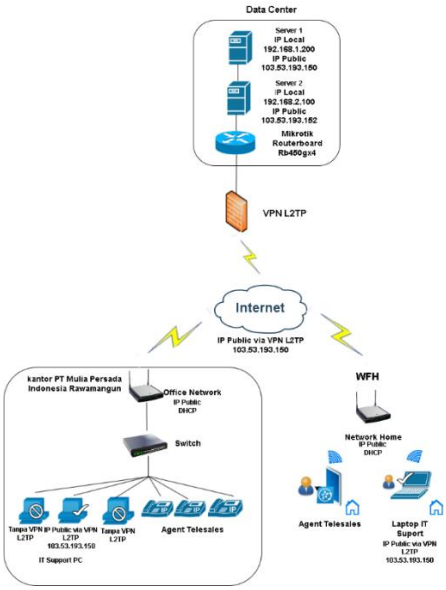
Gambar 3. Topologi jaringan VoIP server dengan VPN L2TP PT Mulia Persada Indonesia

Untuk keamanan jaringan yang diterapkan dalam perancangan VPN L2TP pada server *Randomize number* PT Mulia Persada Indonesia adalah dengan mengintegrasikan antara *cloud computing* melalui server yang ada di *data center* dengan jaringan LAN yang terdapat di kantor serta jaringan internet lainnya ketika IT *Support* sedang WFH atau sedang tidak berada dikantor sehingga server bisa diakses di manapun serta kapanpun dengan jaringan

internet dan perangkat pc atau laptop yang sudah terintegrasi dengan VPN L2TP untuk mempermudah *maintenance* dan pengelolaan server dengan keamanan jaringan yang lebih baik.

3. Skema Jaringan

Dalam upaya untuk meningkatkan keamanan jaringan baik secara internal maupun eksternal, penulis telah mengusulkan dan mengimplementasikan sebuah skema jaringan baru yang memenuhi standar keamanan yang lebih baik dengan VPN L2TP.



Sumber: Penulis (2023)

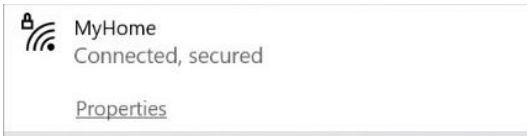
Gambar 4. Skema jaringan VoIP server dengan VPN L2TP PT Mulia Persada Indonesia

4. Keamanan Jaringan

Untuk meningkatkan keamanan jaringan pada server penulis mengusulkan untuk melakukan perancangan dan penerapan VPN L2TP dan ditambah dengan IPSec dengan IP server mikrotik untuk VPN L2TP 103.53.193.150 sebagai keamanan jaringan utama pada server PT Mulia Persada Indonesia sehingga hanya perangkat pc atau laptop yang sudah terintegrasi dengan VPN L2TP yang bisa mengakses server tersebut. Dan perangkat yang diizinkan menggunakan VPN L2TP hanya komputer atau laptop yang digunakan oleh teknisi atau IT *Support* PT Mulia Persada Indonesia.

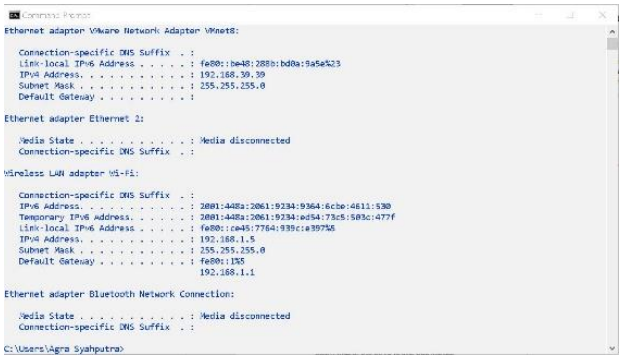
5. Pengujian Jaringan Awal

Pada tahap awal penulis mencoba mengakses server 1 dan server 2 menggunakan jaringan internet WiFi ketika menggunakan *firewall* NAT.



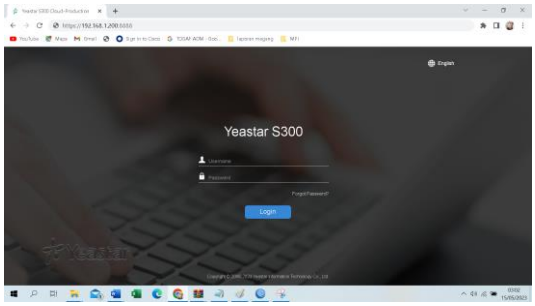
Sumber: Penulis (2023)

Gambar 5. Pengujian Jaringan Awal dengan *firewall* NAT dengan jaringan WiFi



Sumber: Penulis (2023)

Gambar 6. Tampilan IP *config* pada perangkat laptop

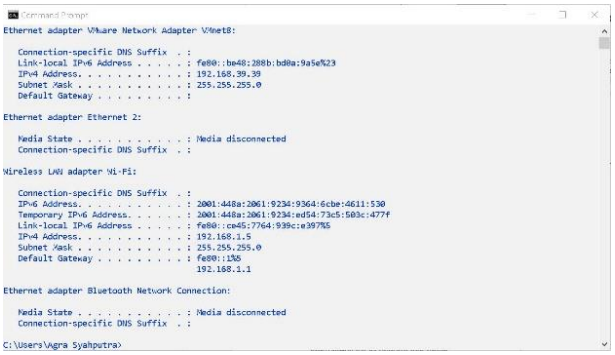


Sumber: Penulis (2023)

Gambar 7. Server berhasil di akses melalui internet dengan *firewall* NAT

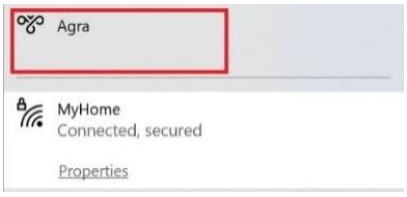
6. Pengujian Jaringan Akhir

Pada pengujian tahap pertama di pengujian akhir penulis mencoba mengakses server tanpa menggunakan VPN L2TP.



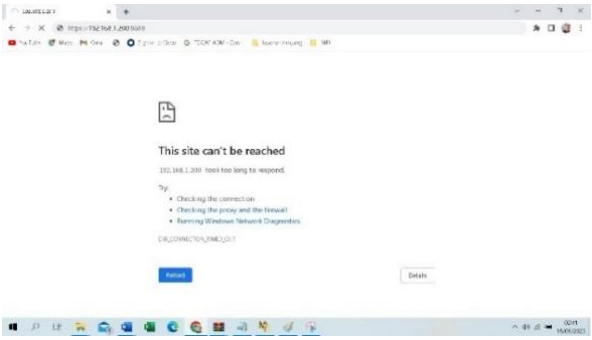
Sumber: Penulis (2023)

Gambar 8. Tampilan IP *config* pada perangkat laptop



Sumber: Penulis (2023)

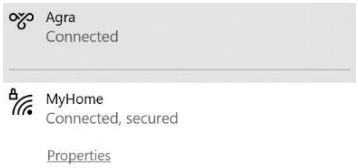
Gambar 9. Pengujian Akses server dengan jaringan WiFi tanpa VPN L2TP



Sumber: Penulis (2023)

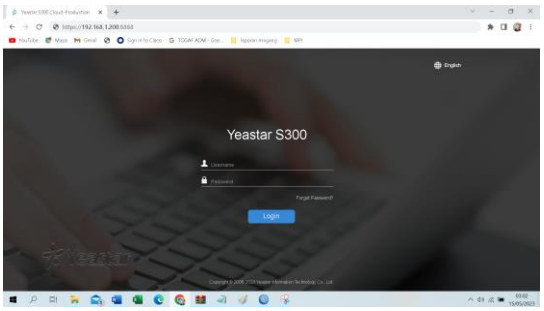
Gambar 10. Akses ke server gagal tanpa VPN L2TP

Hasil pengujian pada server mengalami gagal akses tanpa menggunakan VPN L2TP. Selanjutnya di pengujian tahap kedua penulis mengaktifkan VPN L2TP dan mencoba untuk mengakses Kembali server.



Sumber: Penulis (2023)

Gambar 11. Pengujian Jaringan Akhir dengan VPN L2TP



Sumber: Penulis (2023)

Gambar 12. Akses ke server berhasil dengan VPN L2TP

7. Pengujian *Randomize number*

Contoh penggunaan *randomize number* dengan *softphone linkus* untuk melakukan panggilan keluar ke nomor lain dan nomor akan keluar secara acak.

Sumber: Penulis (2023)

Gambar 13. Pengujian *randomize number*

KESIMPULAN

Setelah melakukan perancangan dan implementasi VoIP server *Randomize number* dengan *firewall* NAT untuk mengubah IP Lokal menjadi IP Publik dengan tujuan agar server bisa diakses dimanapun melalui jaringan internet dengan tujuan mempermudah *maintenance* dan pengelolaan server serta ditambahkan dengan penerapan sistem keamanan VPN L2TP untuk membatasi akses server. Sehingga yang bisa mengakses server tersebut hanya pada perangkat pc dan laptop teknisi atau IT *Support* PT Mulia Persada Indonesia. Untuk meminimalisir terjadinya kebocoran data dan membuat keamanan jaringan dalam server tersebut menjadi lebih baik dari sebelumnya.

Adapun saran yang ingin penulis sampaikan dalam pembahasan yang telah diuraikan pada sistem jaringan VoIP server *Randomize number* PT Mulia Persada Indonesia adalah sebagai berikut. Melakukan perawatan secara berkala pada *hardware* maupun *software* agar performa server dapat tetap berjalan dengan baik, Perangkat yang diizinkan untuk diberi akses VPN L2TP hanya terbatas pada perangkat pc atau laptop IT Support agar keamanan data server dapat tetap terjaga dengan baik, Selalu melakukan pengecekan dan update secara berkala pada *software* dengan versi terbaru untuk menajaga performa pada sistem server.

REFERENSI

Aldo, D. (2020). *PENGANTAR TEKNOLOGI INFORMASI* (J. Insani, Siti (ed.)). INSAN CENDEKIA MANDIRI. https://www.google.co.id/books/edition/PENGANTAR_TEKNOLOGI_INFORMASI/nzMXEAAAQBAJ?hl=id&gbpv=1&dq=pengertian+internet+aldo+dasril&pg=PA116&printsec=frontcover

Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, *3*(1), 104–114. https://doi.org/10.25299/itjrd.2018.vol3(1).1346

Ayub, M., Maulana, A., & Fauzi, A. (2021). Penerapan *Firewall* Dan Protokol IPSec/L2TP Sebagai Solusi Keamanan Akses Jaringan Publik. *Computer Science (CO-SCIENCE)*, *1*(2), 81–90. https://doi.org/10.31294/coscience.v1i2.435

Ilyas, Y. (2021). *Workbook Mikrotik MTCRE Full Lab* (Y. Ilyas (ed.)). Ilyas, Yastril. https://www.google.co.id/books/edition/Workbook_Mikrotik_MTCRE_Full_Lab/YN1JEAAAQBAJ?hl=id&gbpv=1

Kusuma, G. H. A., & Aditiyo N, C. (2020). Implementasi Voip Elastix Server Pada PT XYZ. *Journal of Informatics and Advanced Computing*, *1*(1), 1–7.

Laksamana, Indra, Syukriadi, Aulia, Indra, Yuliswar, Teddy, Jingga, Trinovita, Z. (2023). *Jaringan Komputer Menggunakan Mikrotik RouterOS* (T. Pena (ed.)). Goresan Pena. https://books.google.co.id/books?id=CgSvEAAAQBAJ&pg=PA91&dq=mikrotik+routeros&hl=id&newbks=#v=onepage&q&f=false

Mufida, E., & Agus Rahayu, D. W. (2018). Pengembangan Sistem VOIP Menggunakan Server Issabel Versi 4.0 dan Tunnel EOIP pada OMNI Hospital Alam Sutera. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *18*(1), 13–20. https://doi.org/10.30812/matrik.v18i1.330

Nanda, R. (2021). *VoIP Telephony and You*. https://www.google.co.id/books/edition/VoIP_Telephony_and_You/VmotEAAAQBAJ?hl=en&gbpv=1

Rahino, B. G., & Susila, A. (2022). *Implementasi Jaringan VPN (L2TP / IPSec) Mikrotik Untuk Remote Access Sebagai Security Selama Work From Home*. *1*(11), 1911–1918.

Tahir, M. (2022). *PENGANTAR JARINGAN KOMPUTER DASAR* (S. Imanda (ed.)). CV. Literasi Nusantara Abadi. https://www.google.co.id/books/edition/PENGANTAR_JARINGAN_KOMPUTER_DASAR/4DmqEAAAQBAJ?hl=id&gbpv=1&dq=pengertian+keamanan+jaringan+komputer&pg=PA97&printsec=frontcover

Triyansa, F., & Sobari, I. A. (2022). Implementasi Jaringan VPN Menggunakan L2TP Dengan IP Sec Pada PT Datindo Infonet Prima. *Computer Science (CO-SCIENCE)*, *2*(2), 82–89. https://doi.org/10.31294/coscience.v2i2.1168

Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, *8*(3), 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

Zackiansyah, Azrial, A. (2022). *Easy and Practice PPPoE Server, VPN PPTP, Bandwidth Management, Mikrotik Hotspot with Mikrotik RouterBoard* (G. Ryan, Mikha, Raymond (ed.)). CV. XP Solution. https://www.google.co.id/books/edition/Easy_and_Practice_PPPoE_Server_VPN_PPTP/XP18EAAAQBAJ?gbpv=1