OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

Implementasi Jaringan VPN (L2TP/Ipsec) Mikrotik Untuk *Remote Access* Sebagai *Security* Selama *Work From Home*

Bayu Gagat Rahino[1], Atang Susila[2*]

[1,2]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]bayugagat@hotmail.com, 2atang.g66@gmail.com
(* : coressponding author)

Abstrak−Selama pandemi COVID-19, PT XL Axiata menerapkan kebijakan work from home, yang mengharuskan karyawan untuk dapat terhubung ke jaringan dan data perusahaan menggunakan internet atau jaringan publik. Penyadapan oleh orang yang tidak berwenang menjadi lebih mungkin terjadi saat menggunakan jaringan publik. Karyawan PT XL Axiata tbk dapat terhubung ke jaringan dan data perusahaan menggunakan jaringan publik dengan aman dan mudah menggunakan VPN sebagai solusi keamanan. Jaringan pribadi virtual (VPN) menyediakan koneksi jarak jauh yang aman bagi klien untuk bertukar informasi dengan jaringan perusahaan. Penelitian ini berkaitan dengan L2TP/IPSec-VPN yang menghubungkan intranet perusahaan. Jaringan L2TP/IPSec-VPN diimplementasikan dengan protokol keamanan untuk manajemen kunci dan pertukaran, otentikasi, dan integritas menggunakan perangkat virtual dengan bantuan program *Vmware Workstation*. Pengujian dan verifikasi analisis paket data dilakukan menggunakan perintah PING di command prompt dan Wireshark untuk memastikan enkripsi data paket selama pertukaran data antara jaringan yang berbeda milik perusahaan yang sama. Metodologi yang digunakan dalam penelitian ini adalah mengumpulkan data melalui survei dan wawancara, kemudian menganalisis jaringan yang ada saat ini dan kebutuhan akan dukungan desain jaringan. dalam rangka meningkatkan produktivitas dan kinerja karyawan saat bekerja dari rumah, serta mampu bersaing dengan bisnis lain di pasar yang semakin kompetitif.

Kata Kunci: Jaringan Publik, Pandemi, VPN, Vmware Workstation, L2TP/IPSec

Abstract− *During the COVID-19 pandemic, PT XL Axiata implemented a work from home policy, which requires employees to be able to connect to the company's network and data using the internet or public networks. Wiretapping by unauthorized persons becomes more likely when using public networks. Employees of PT XL Axiata tbk can connect to the company's network and data using public networks safely and easily using VPN as a security solution. A virtual private network (VPN) provides a secure remote connection for clients to exchange information with the corporate network. This research is related to L2TP/IPSec-VPN connecting corporate intranet. The L2TP/IPSec-VPN network is implemented with security protocols for key and exchange management, authentication, and integrity using virtual devices with the help of the Vmware Workstation program. Data packet analysis testing and verification is performed using the PING command at the command prompt and Wireshark to ensure packet data encryption during data exchange between different networks belonging to the same company. The methodology used in this research is to collect data through surveys and interviews, then analyze the current network and the need for network design support. in order to increase employee productivity and performance while working from home, as well as being able to compete with other businesses in an increasingly competitive market.*

Keywords: *Public Network, Pandemic, VPN, Vmware Workstation, L2TP/IPSec*

1. PENDAHULUAN

Dalam jaringan komputer, keamanan merupakan faktor penting yang harus diperhatikan. Sistem keamanan ini dapat terdiri dari kemampuan untuk mengidentifikasi dan menghentikan serangan penyerang (penyusup). Masalah serangan yang terjadi Penyerang dapat menggunakan port terbuka seperti telnet, ftp, dan lainnya untuk melakukan pemindaian *port* dalam jaringan komputer dan mendapatkan akses ke sistem (Alamsyah, Hendri 2020). Sejak wabah COVID-19 melanda sejak bulan Maret 2019 di Indonesia, diberlakukannya sosial distancing atau pembatasan jarak dan aktivitas diluar rumah. Bekerja dari rumah menjadi solusi bagi PT XL Axiata Tbk, karena sebagai salah satu provider terbesar di Indonesia harus tetap meningkatkan pelayanan dan kenyamanan pelanggan. Internet merupakan salah satu teknologi yang saat ini berkembang sangat cepat. Jaringan publik atau biasa kita sebut dengan internet dapat diakses oleh setiap penggunanya untuk bertukar informasi dan data. Di setiap perusahaan dipastikan setiap aktivitas penggunaan internetnya dimanfaatkan untuk bertukar informasi dan data. Namun, penggunaan jaringan publik untuk

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

mengakses perangkat jaringan perusahaan dinilai kurang aman, karena menggunakan jaringan publik rentan terhadap pencurian data oleh pihak yang tidak berwenang.

Maka untuk mengatasi masalah tersebut perlu dirancang sebuah jaringan *Virtual Private Network* (VPN) dengan metode *tunneling mode* menggunakan *Layer* 2 *Tunneling Protocol* (L2TP) yang dikombinasikan dengan IPSec (*Internet Protocol Security*) dan Mikrotik. Pada dasarnya VPN merupakan jaringan pribadi yang bersifat *private* (tidak dapat diakses untuk umum) namun tetap menggunakan akses jaringan internet untuk menghubungkan remote perangkat jaringan dengan aman dan efisien. Terdapat kombinasi enkripsi dan *tunneling* sebagai solusi untuk mengatasi masalah keamanan dalam jaringan.

Saat ini PT XL Axiata Tbk menerapkan *Hybrid Working* yang artinya karyawan bisa bekerja di berbagai tempat tanpa harus terbelenggu waktu termasuk bekerja dari rumah (*Work from Home*), karena tidak memungkinkan karyawan untuk datang terlebih dahulu untuk mengakses jaringan lokal perusahaan dengan adanya penerapan kebijakan pembatasan aktivitas diluar rumah. Hal ini menyebabkan masalah bagi perusahaan karena belum ada akses secara remote ke dalam jaringan perusahaan, khususnya bagi karyawan yang saat ini sedang bekerja dari rumah.

Virtual Private Network (VPN) adalah metode terbaik untuk menyediakan layanan yang tersebar melalui arsitektur jaringan publik. VPN menawarkan harga yang terjangkau, penggunaan bandwidth yang efektif, fungsionalitas yang dapat diskalakan dan fleksibel, serta koneksi pribadi dan aman. Jaringan pribadi virtual (VPN) menawarkan keamanan tunneling untuk lalu lintas jaringan untuk melewati antara dua node jaringan. Sistem operasi, perangkat keras yang digunakan, kompatibilitas, dan algoritma yang digunakan semuanya berdampak pada jaringan VPN.

VPN dapat dikategorikan berdasarkan risiko keamanan yang terkait dengan tunneling, lokasi titik akhir, opsi konektivitas, kekuatan tindakan keamanan, dan jenis protokol *tunneling* yang berbeda. Koneksi VPN dibuat melalui terowongan, media virtual antara dua *node* yang mungkin berada di jaringan yang berbeda.

Dari penelitian sebelumnya dipelajari dan didapatkan tentang beberapa jenis protokol tunneling yang diperuntukan sebagai *remote access*, diantaranya *Point to Point Tunneling Protocol* (PPTP) (ISSN, 2657-0793), *Layer* 2 *Tunneling Protocol* (L2TP) (ISSN: 2354-5771), *Internet Protocol Security* (IPSec) (p-ISSN: 2406-773). Berdasarkan penjelasan permasalahan diatas, maka diperoleh judul "IMPLEMENTASI JARINGAN VPN (L2TP/IPSEC) MIKROTIK UNTUK *REMOTE ACCESS* SEBAGAI *SECURITY* SELAMA *WORK FROM HOME"* dengan solusi yang diusulkan untuk membangun sistem yang aman dalam mengakses jaringan perusahaan saat bekerja dari rumah.

2. METODOLOGI PENELITIAN

2.1 Pengumpulan data

a. Studi Kepustakaan
   Dengan mengumpulkan data dan informasi tentang teknologi jaringan dan yang berkaitan dengan VPN yang berasal dari beberapa buku referensi, jurnal ilmiah, internet, dan sumber-sumber yang berkaitan.
b. Studi Lapangan
   Pengumpulan data dan informasi berkaitan dengan jaringan dan keamanan jaringan yang saat ini digunakan oleh perusahaan dengan melakukan observasi langsung dan wawancara dengan pihak PT XL Axiata.

2.2 Analisis Jaringan

Data dan informasi yang telah dikumpulkan, selanjutnya dianalisis untuk mengetahui kinerja jaringan yang digunakan perusahaan sebelum menggunakan VPN.

2.3 Perancangan Sistem Jaringan

a. Membuat perancangan yang dibutuhkan berdasarkan analisis, hasil observasi, dan pengumpulan data.
b. Merancang jaringan VPN yang telah diusulkan dengan mengkonfigurasi simulasi yang sudah ada.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

2.4 Implementasi Jaringan VPN

Mengimplementasikan simulasi jaringan VPN yang telah dirancang dan diusulkan sebelumnya.

2.5 Pengujian dan evaluasi jaringan VPN

Dilakukan pengujian jaringan VPN atau non-VPN dengan bantuan *software Wireshark* untuk menunjukan hasil penggunaan VPN dalam jaringan yang sudah di implementasi berupa simulasi di *VMware Workstation.*

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

3.1.1 Analisa Kebutuhan *Hardware*

Hardware adalah setiap peralatan atau komponen komputer yang dapat langsung disentuh dan diamati dengan mata telanjang dianggap sebagai. Oleh karena itu perangkat keras merupakan komponen dengan bentuk fisik. Hardware yang dibutuhkan antara lain:

a. Laptop HP Pavilion *Gaming*
b. *Mouse*

3.1.2 Analisa Kebutuhan *Software*

Perangkat lunak atau *software* adalah data yang telah diformat, disimpan, dan diprogram secara digital untuk tujuan tertentu. Perangkat ini dapat dikendalikan menggunakan perangkat komputer dan tidak memiliki bentuk fisik. Perangkat lunak yang digunakan dalam penelitian ini sebagai berikut:

a. Sistem operasi : *Windows 10 & Ubuntu Server*
b. Virtualisasi & Simulasi: *Vmware Workstation*
c. Network Analyzer : *Wireshark*
d. *Monitoring* : *Telegram & Winbox*

3.1.3 Analisa Jaringan yang sedang berjalan

Jaringan komputer yang digunakan di PT. XL Axiata adalah jenis jaringan LAN (*Local Area Network*), yang merupakan sistem yang terdiri dari komputer, perangkat lunak, dan perangkat jaringan lainnya yang bekerja sama untuk mencapai tujuan bersama. Agar mendapatkan hasil yang sama, setiap komponen jaringan komputer membuat permintaan layanan dan menawarkannya (*service*). Pengguna (*client*) adalah orang yang meminta atau mendapatkan layanan, dan penyedia (*service*) adalah pihak yang memberi atau mengirim layanan (*server*).

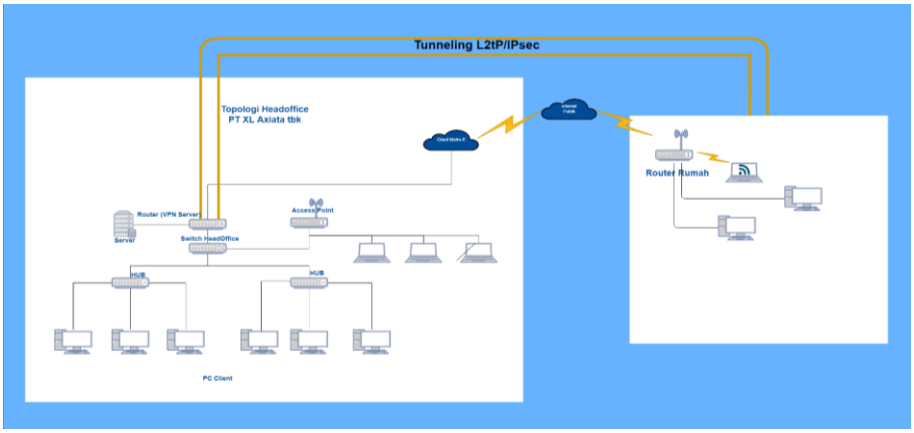
3.1.3.1 Arsitektur Jaringan

Arsitektur jaringan yang digunakan pada PT XL Axiata tbk adalah sistem operasi jaringan LAN (*Local Area Network*), sesuai dengan penelitian penulis pada PT XL Axiata tbk. Sistem operasi jaringan LAN memungkinkan pengguna untuk saling terhubung jika memiliki *host ID* yang sama karena PT XL Axiata tbk terhubung ke alamat IP dan memiliki *host ID* yang berbeda alamat IP harus didaftarkan terlebih dahulu di dalam *router* untuk terhubung ke alamat IP tujuan.

3.2 Perancangan Topologi Jaringan VPN L2TP/IPSec

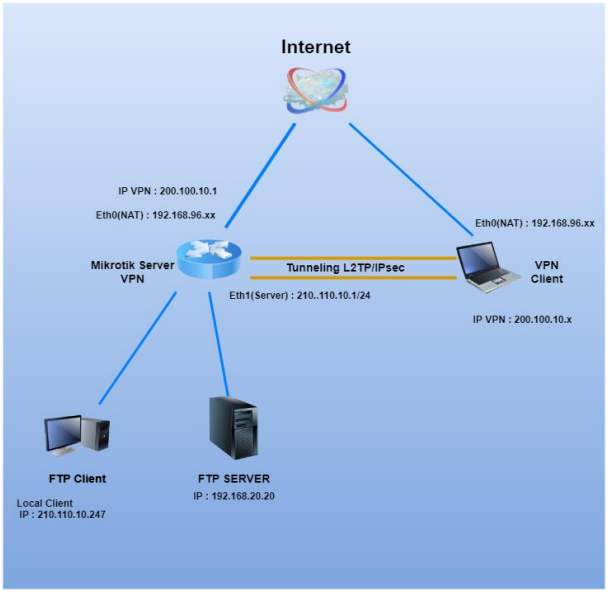
Topologi di PT XL Axiata kurang lebih sama seperti pada gambar berikut, kecuali fitur seperti *Virtual Private Network* dengan *Remote Access* berbasis L2TP *(Layer 2 Tunneling Protocol*) dan *Internet Protocol Security*. Penulis mencoba menarik kesimpulan bahwa secara keseluruhan tidak perlu adanya perubahan topologi pada PT XL Axiata.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918



Gambar 1. Rancangan Jaringan Simulasi

3.2.1 Perancangan Topologi Simulasi Jaringan



Gambar 2. Topologi Jaringan Simulasi

Dalam gambar 3 dijelaskan bahwa topologi jaringan simulasi dengan *Vmware Workstation* yang diusulkan, dengan penggunaan vpn sebagai *remote access* dan *virtual router* mikrotik yang digunakan sebagai VPN *server*. Dalam rancangan VPN ini mikrotik berperan khusus sebagai pencipta tunnel untuk menjamin keamanan dalam pertukaran data antara pengguna dan *server*.

Rancangan gambar diperoleh dari hasil identifikasi masalah, dimana kebutuhan karyawan yang sedang bekerja dari rumah atau *Work from Home* dapat mengakses jaringan dan data perusahaan dengan aman. Mikrotik *router* OS sebagai vpn *server* yang menggunakan teknologi VPN untuk menghubungkan *client* dan VPN *server*, berada pada baris terdepan jaringan perusahaan. Koneksi *point-to-point* dapat terjadi setelah *tunnel* dibuat. Untuk menjaga keamanan tersebut, *tunnel* dilengkapi dengan mekanisme enkripsi dalam implementasinya. Di mana data terenkripsi hanya dapat dilihat setelah didekripsi oleh *server* atau VPN *client*.

Mobile user merupakan setiap karyawan yang saat pandemi diharuskan bekerja dari rumah. *User* terhubung ke jaringan pusat perusahaan menggunakan VPN *client* dengan jaringan publik atau internet untuk menjamin keamanannya. Gambar 2 menunjukkan bagaimana koneksi VPN dibuat melalui jaringan internet. Analoginya untuk membangun jaringan VPN yang terhubung ke *internet* yang seolah-olah itu berada di jaringan lokal. Oleh karena itu, membangun koneksi virtual memerlukan koneksi khusus antara *server* dan *client*.

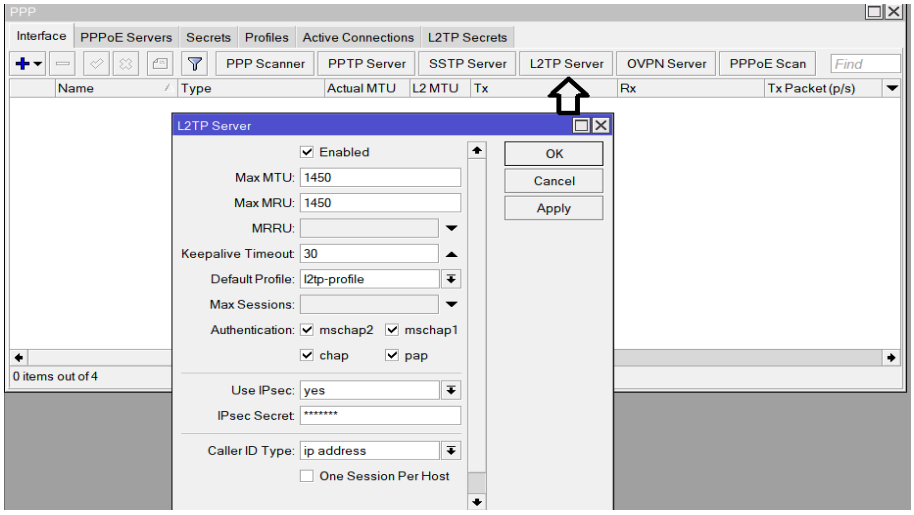
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

4. IMPLEMENTASI

4.1 Implementasi

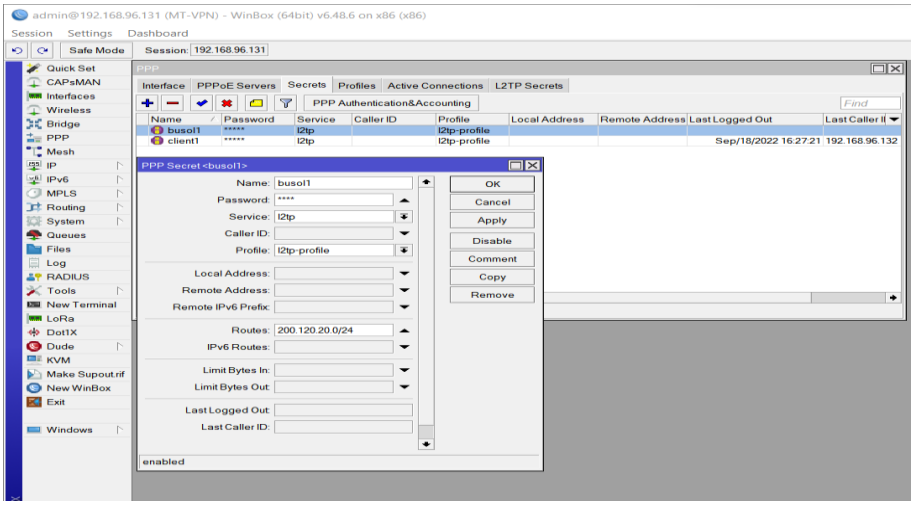
Implementasi jaringan VPN adalah ketersediaan jaringan dalam memberikan pelayanan akses melalui internet pada *router* kantor pusat sebai VPN *Server* dan VPN *Client* hanya konfigurasi untuk koneksi ke VPN *Server*. Sehingga pada VPN *Client* dapat terhubung kedalam jaringan kantor pusat. Berikut ini adalah implementasi jaringan VPN yang dibuat:

4.1.1 Konfigurasi L2TP/IPsec



Gambar 3. Mengaktifkan L2TP *Server*:

Pilih menu L2TP *Server* hingga muncul kotak dialog L2TP *Server* pada kotak dialog PPP, seperti pada gambar 4 Proses konfigurasi *server* L2TP digambarkan sebagai berikut pada 4 buka tab L2TP *server* dan *ceklist* pada tab "*Enabled*", lalu pilih profil default yang terisi dengan "*l2tp-profile*", Use *Ipsec* pilih *yes*, kemudian masukan *Ipsec Secret*nya.

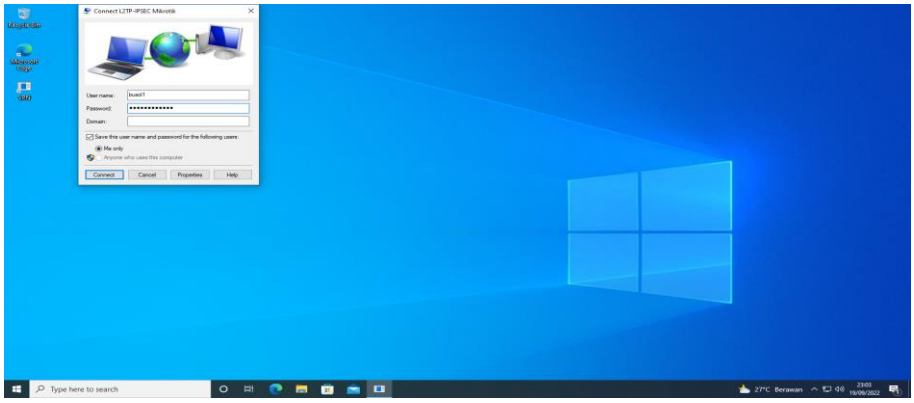


Gambar 4. *Add PPP Secret*:

Pilih *secret tab*, lalu tekan Tambah [+]. Di sini, isi beberapa parameter umum utama yang diperlukan untuk membuat koneksi. Masukan "*Name & Password*" untuk koneksi *dial up* L2TP dari *client*. Setelah itu, "L2TP" atau "*any*" untuk semua jenis layanan PPP dapat digunakan untuk mengisi pada bagian *Service*. *Setting IP route* "**200.120.20.0/24**". Ketika koneksi L2TP dibuat dan digunakan sebagai *gateway* komunikasi data, alamat IP ini akan ditambahkan secara otomatis.

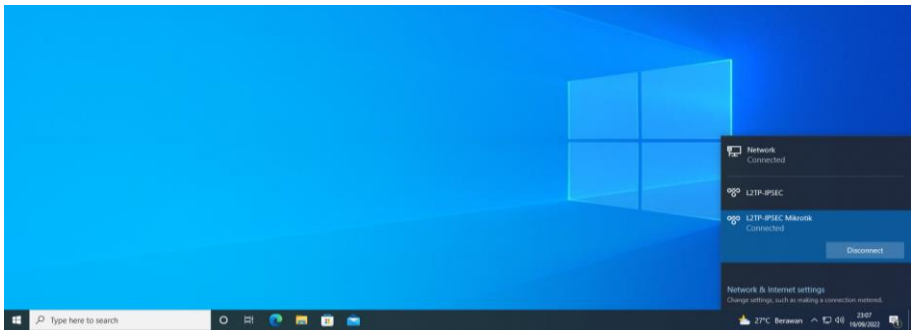
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

4.1.2 Koneksi VPN Client ke VPN Server



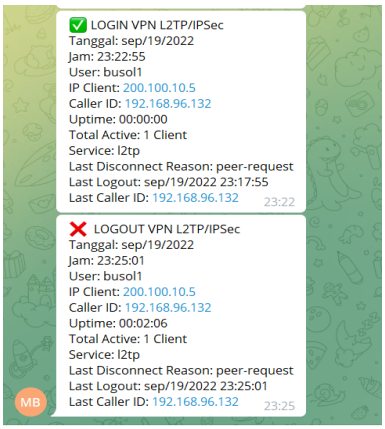
Gambar 5. Koneksi ke L2TP-IPSec Mikrotik:

Pada tampilan seperti pada gambar 6 ketikan pada *tab Username and password* karena kita *login* vpn menggunakan *username* dan *password* yang sudah kita buat sebelumnya berikut adalah "username(optional): busol1 password(optional). *Save this username and password for the following users*: beri *ceklist* jika *username* dan *password* ingin disimpan. Setelah konfigurasi selesai, lalukan *dial-up* pada *profile vpn* yang sudah kita buat tadi dengan klik *Connect* untuk menghubungkan.



Gambar 6. Koneksi VPN Berhasil

Jika koneksi berhasil, tampilan akan terlihat seperti gambar 7. Setelah itu, layanan koneksi VPN dengan model L2TP/Ipsec dapat digunakan.

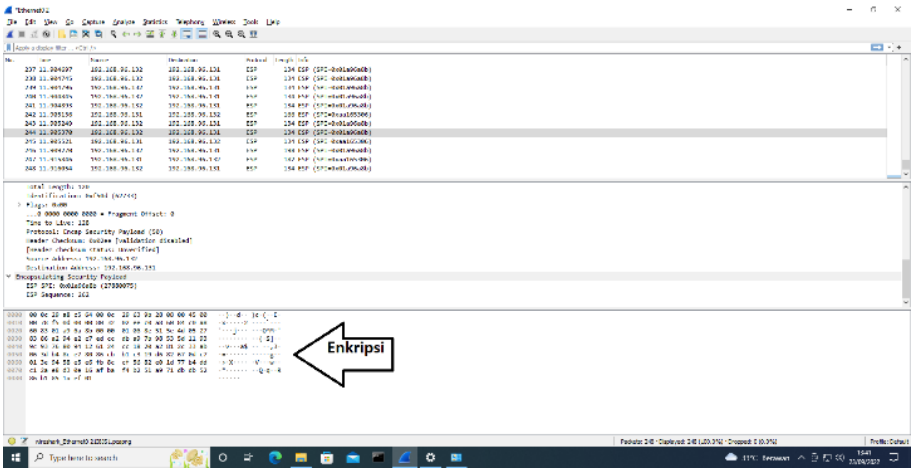


Gambar 7. Notifikasi Login & Logout Bot Telegram

Pada gambar 7. notifikasi bot telegram ini berfungsi sebagai *monitoring*, siapa saja pengguna atau *user* vpn yang sedang terhubung dalam jaringan perusahaan.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1911-1918

4.2 Testing



Gambar 8. Enkripsi Data Customer dalam jaringan L2TP/IPsec:

Dengan menggunakan VPN L2TP/Ipsec terlihat pada aplikasi *Wireshark*, protokol ESP (*Encapsulating Security Payload*). *File Data Customer*(.xlsx) tidak dapat dapat terbaca isinya, file tersebut sudah terenkripsi. Membuktikan bahwa menggabungkan IPSec sebagai keamanan pada L2TP sangatlah baik.

5. KESIMPULAN

Setelah melakukan uji coba serta simulasi sistem jaringan menggunakan *Vmware Workstation* seperti yang sudah dijelaskan pada bab sebelumnya, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Jaringan berbasis *Remote Access* VPN L2TP/Ipsec dapat terhubung menggunakan sistem operasi *windows* dan berfungsi baik saat proses simulasi sehingga dengan adanya sistem ini, dapat menghubungkan karyawan yang sedang *work from home*.
b. Sistem keamanan dengan protokol L2TP/Ipsec sudah berjalan sesuai dengan yang diinginkan dengan melakukan enkripsi dan dekripsi.
c. Autentikasi akses client kedalam vpn dengan menggunakan L2TP/Ipsec dapat dilakukan dengan membuat sebuah koneksi *dial-up* baru dan memasukkan *username* dan *password* yang sudah terdaftar pada *router* sebagai VPN *Server*, dan juga memasukkan sebuah kata kunci IPSec yang dibuat pada VPN *server*.
d. *Administrator* dapat memonitor *client* yang terhubung pada jaringan VPN dengan aplikasi Telegram.

REFERENCES

Forouzan, B. A. (2010). TCP/IP Protocol Suite. 4th Ed. New York: McGraw-Hill. ISBN:9780071084208 Network Security,Brenton,Cris, Hunt, Cameron

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point to Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains Dan Manajemen*, *8*(1), 128–139. https://doi.org/10.31294/evolusi.v8i1.7658

Erawati, W., & Heristian, S. (2018). Implementasi Virtual Private Network (Vpn) Menggunakan Protokol Pptp Mikrotik Router. *Jurnal Teknik Informatika STMIK Antar Bangsa*, *IV* (1), 28. http://ejournalab.com/index.php/jti/issue/view/14/showToc

Ikhwan, S., & Amalina, A. (2017). Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus: Dinhubkominfo Kabupaten Banyumas). *Jurnal Infotel*, *9*(3), 265–270.

Maryanto, M., Maisyaroh, M., & Santoso, B. (2018). Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data. *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic*, *6*(2), 179–188.

Pratama, H., & Puspitasari, N. F. (2021). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. Creative Information Technology *Journal*, *7*(1), 51. https://doi.org/10.24076/citec.2020v7i1.253

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology*, *3*(2), 260–267.

Sari, A. P., Sulistiyono, & Kemala, N. (2020). Perancangan Jaringan Virtual Private Network Berbasis IP Security Menggunakan Router Mikrotik. *Jurnal PROSISKO*, *7*(2), 150–164.

Siahaan, E. S. P., & Suharyanto, C. E. (2021). *Perancangan Dan Implementasi Virtual Private Network Dengan Mikrotik. Computer and Science.*

Umaroh, L., & Rifauddin, M. (2020). Implementasi Virtual Private Network (Vpn) Di Perpustakaan Universitas Islam Malang. Baca: *Jurnal Dokumentasi Dan Informasi*, *41*(2), 193. https://doi.org/10.14203/j.baca.v41i2.531

Zarkasyi, M. H., Agus, I., Permana, G., Dillak, H. C., & Kom, S. (2018). Implementasi Virtual Private Network (Vpn) Server Dengan Menggunakan Mikrotik Os Di Pt. Charisma Persada Nusantara Implementation of Virtual Private Network (Vpn) Server Using Mikrotik Os in Pt. Charisma Persada Nusantara. In Implementasi Virtual Private Network (VPN) Server dengan Menggunakan Mikrotik Os di Pt. Charisma Persada Nusantara (Vol. 4, Issue 3). https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/7401

Aristiani, O. (2019). *PERANCANGAN VPN DENGAN METODE L2TP DAN IPSEC PADA PT KAWASAN MARGOREJO PERSADA BANDUNG*.

Zamalia, W.O., Aksara, L.F., & Yamin, M. (2018). *ANALISIS PERBANDINGAN PERFORMA QOS, PPTP, L2TP, SSTP DAN IPSEC PADA JARINGAN VPN MENGGUNAKAN MIKROTIK.*

Wicaksana, P., Hadi, F., & Hadi, A.F. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*

Alamsyah, Hendri (2022). *Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System*