Protokol L2TP dan IPsec Sebagai Keamanan Jaringan Pada Dinas Kominfotik Sumatera Barat

Ridho Laksamana[1], Emil Naf'an[2], Eka Praja Wiyata Mandala[3]

[a] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang
Jl. Raya Lubuk Begalung, Lubuk Begalung Nan XX, Kec. Lubuk Begalung, Kota Padang, Sumatera Barat 25122
[1] ridholaksamana1@gmail.com; [2] emilnafan@upiyptk.ac.id; [3] ekaprajawm@upiyptk.ac.id
*Penulis Korespondensi

ABSTRAK

Beberapa masalah muncul pada beberapa perusahaan-perusahaan baik itu dalam skala besar maupun skala kecil. Adapun dari berbagai macam masalah yang terjadi, salah satunya adalah masalah keamanan jaringan komputer. Pada Kantor Dinas Komunikasi, Informatika dan Statistik Sumatera Barat terdapat masalah keamanan jaringan, salah satunya masalah yang sering terjadi yaitu serangan dari berbagai macam *malware.* Salah satu solusi untuk mengatasi masalah tersebut ialah dengan menggunakan teknologi keamanan jaringan *VPN (Virtual Private Network)* dengan metode *L2TP (Layer 2 Tunneling Protocol)* dan metode *IPSec (Internet Protocol Security)* yang akan digunakan sebagai alternatif keamanan jaringan untuk meningkatkan keamanan pertukaran data perusahaan. Penelitian ini membuat jaringan *private* dengan menggunakan *IP* publik yang dikonfigurasikan pada mikrotik dan konfigurasi dibuat untuk meminimalkan biaya dan waktu implementasi. Protokol *L2TP (Layer 2 Tunneling Protocol)* dan *IPSec (IP Security)* mampu mengatasi serangan *DDoS attack* sehingga *server* tidak mudah *down* saat terindikasi serangan.

.

Kata Kunci
Virtual Private Network (VPN)
Layer 2 Tunneling Protocol (L2TP)
IP Security (IPSec)
MikroTik.

1. Pendahuluan

Kantor Dinas Komunikasi Informatika dan Statistik Provinsi Sumatera Barat merupakan salah satu kantor yang memanfaatkan teknologi elektronika, komputerisasi, serta jaringan komputer dalam proses kegiatan sehari-hari. Beberapa masalah muncul pada beberapa perusahaan-perusahaan baik itu dalam skala besar maupun skala kecil. Adapun dari berbagai macam masalah yang terjadi, salah satunya adalah masalah keamanan jaringan komputer. Pada Kantor Dinas Komunikasi, Informatika dan Statistik Sumatera Barat terdapat masalah keamanan jaringan, salah satunya masalah yang sering terjadi yaitu serangan dari berbagai macam malware. Serangan yang terjadi dapat saja muncul dari internet atau pun seorang *attacker* yang mencoba untuk membobol keamanan jaringan pada Dinas Komunikasi, Informatika dan Statistik Sumatera Barat yang hanya menggunakan sistem keamanan *firewall* untuk mengatasi serangan dari malware tersebut.

Penelitian ini dengan menggunakan teknologi keamanan jaringan VPN (Virtual Private Network) dengan metode *L2TP (Layer 2 Tunneling Protocol)* dan metode *IPSec (Internet Protocol Security)* yang akan digunakan sebagai alternatif keamanan jaringan dengan memberikan gambaran simulasi. *L2TP* dan *IPSec* diharapkan bisa meningkatkan keamanan pertukaran data perusahaan. Karena proses kerja *VPN* membuat jaringan sendiri yang sifat nya rahasia dengan menggunakan *IP* publik dan menjadikan keamanan data lebih terjaga kerahasiaan nya serta mencegah kebocoran data dari pihak-pihak yang tidak bertanggung jawab.

Protokol jaringan komputer merupakan sekumpulan keputusan yang mengizinkan satu komputer untuk bertukar data dengan komputer lain.[1] Sebuah jaringan komputer dihubungkan melalui media transmisi yang memakai kabel maupun nirkabel.[2] Tujuan dari jaringan komputer berguna sebagai media informasi dari data yang dibawa pengirim *(transmitter)* dapat sampai kepada penerima *(receiver)* dengan tepat.[3] Komputer yang menerima bantuan disebut *client* dan yang mengirimkan bantuan disebut *server.*[4] Keamanan jaringan komputer mengarah pada perangkat lunak, perangkat keras dan perangkat lainnya yang terdapat pada suatu komputer itu sendiri.[5] Beberapa upaya diperlukan dalam

pencegahan mengurangi resiko terjadinya serangan dan aktivitas yang mengganggu masuk kedalam jaringan komputer.[6] *Firewall* adalah algoritma yang memungkinkan aktivitas penyaringan untuk memungkinkan akses ke akses jaringan publik dan untuk menentukan pembatasan akses untuk komputer yang tidak dapat melewati akses jaringan publik yang biasa disebut dengan *filtering*.[7]

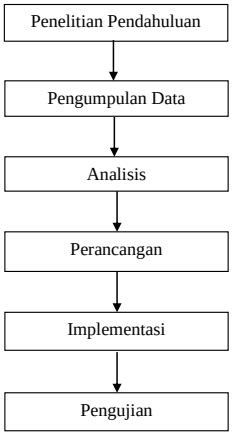
Virtual Private Network (VPN) dikenal dengan sebutan pengaman privasi yang memudahkan terkoneksi dan berkomunikasi antara jaringan publik dan jaringan lokal. *VPN* tidak diberikan keterangan oleh *router*, tetapi dinyatakan oleh mekanisme keamanan dan prosedur-prosedur yang hanya diberi akses *VPN* dan informasi yang meluncur melaluinya.[8] *Virtual Private Network (VPN)* dengan metode *L2TP* menghasilkan peningkatkan keamanan jaringan dan dapat memudahkan akses berkas yang berbeda lokasi.[9] *VPN* dengan memanfaatkan protokol *IPSec* digunakan sebagai autentkasi sistem keamanan jaringan.[10]

Protokol Point to Point Tunneling Protocol (PPTP) memungkinkan keamanan dalam mengirim data melalui kontrol client (jarak jauh) ke server suatu kantor dengan adanya Virtual Private Network (VPN) melalui TCP/IP.[11] L2TP (Layer 2 Tunneling Protocol) dikenal dengan nama protokol dial-up virtual. IPSec juga dikenal sebagai sebuah kemanan terbuka yang dikembangkan oleh Internet Engineering Task Force (IETF). IPSec (IP Security) diterapkan pada lapisan transport dalam OSI Reference Model yang bertujuan melindungi protokol IP (Internet Protocol) dan protokol-protokol lebih aman dengan memanfaatkan beberapa strategi keamanan yang dapat dirancang untuk mencapai keamanan pemanfaatan jaringan komputer. [12]

Alamat IP (IP Address) dikenal sebagai lokasi yang dibagikan ke jaringan sebagai perangkat jaringan yang menggunakan protokol TCP/IP.[13] Mikrotik router OS merupakan Operating System perangkat lunak yang dibentuk khusus pada jaringan router. Mikrotik Router dikembangkan dari kernel linux dan didesain dengan tujuan memberikan kemudahan kepada pengguna nya. Manajemen bisa dilakukan dengan menggunakan aplikasi winbox.[14] Mikrotik memberi service terhadap ISP untuk penggunan bantuan saluran internet di seluruh dunia.[15]

2. Metodologi Penelitian

Penelitian ini menggambarkan tahapan-tahapan dari konsep yang akan dilakukan dalam penelitian. Adapun tahapan dari penelitian ini dapat dilihat pada Gambar 1 berikut ini:



Gambar 1 Kerangka Penelitian

Penelitian pendahuluan dilakukan untuk mengamati atau mengidentifikasi secara langsung apa saja permasalahan yang menjadi acuan utama penulis memilih tempat ini sebagai objek penelitian. Adapun hal yang penulis amati adalah permasalahan keamanan jaringan komputer yang sering dialami oleh objek. Pada Kantor Dinas Komunikasi, Informatika dan Statistik Sumatera Barat terdapat masalah keamanan jaringan, salah satunya masalah yang sering terjadi yaitu serangan dari berbagai macam *malware*. Adapun metode penelitian yang dilakukan oleh penulis dalam menyelesaikan penelitian ini adalah sebagai berikut:

2.1.1. Penelitian Lapangan (Field Research)

Penelitian yang dilakukan dengan cara mengunjungi langsung tempat penelitian. Penelitian lapangan ini dilakukan dengan tahapan sebagai berikut:

Jurnal Sarjana Teknik Informatika
Vol. 10., No. 3, Oktober 2022, pp. 162-171

- Observasi

Dalam tahapan observasi ini, penulis mengumpulkan data yang diperoleh dengan cara melakukan pengamatan langsung di Kantor Dinas Komunikasi, Informatika dan Statistik Sumatera Barat.

- Wawancara

Penulis melakukan wawancara dengan Seksi Infrastruktur Jaringan TIK Dinas komunikasi, Informatika dan Statistik. Penulis melakukan sesi tanya jawab dengan beberapa pertanyaan yang berkaitan dengan penelitian yang penulis lakukan.

2.1.2. Penelitan Pustaka (Library Research)

Study Literatur pada penelitian ini dilakukan dengan cara membaca, memahami, serta menyimpulkan dari berbagai sumber baik buku-buku, arsip maupun berbagai jurnal yang berhubungan dengan tema dalam penelitian ini. Sehingga pada penelitian ini memiliki informasi yang dapat dijadikan rujukan dalam memperkuat argumentasi yang ada pada penelitian yang dilakukan.

2.2. Analisis

Berdasarkan beberapa idenfikasi masalah setelah melakukan pengumpulan data dari buku, jurnal, artikan dan informasi-informasi wawancara akan dilakukan analisis dengan tujuan memecahkan masalah dan menemukan solusi.

2.3. Perancangan Sistem

Dalam hal ini memberikan gambaran dalam pembuatan perancangan jaringan Protokol *L2TP* dan *IPSec*. Adapun perancangan yang akan dilakukan dalam penelitian berdasarkan dari data-data yang dikumpulkan melalui kunjungan ke tempat penelitian dan konsultasi langsung dengan bagian IT dari tempat penelitian. Perancangan akan dibuat dalam bentuk topologi jaringan dan konfigurasi kemanan jaringan komputer.

2.4. Implementasi Sistem

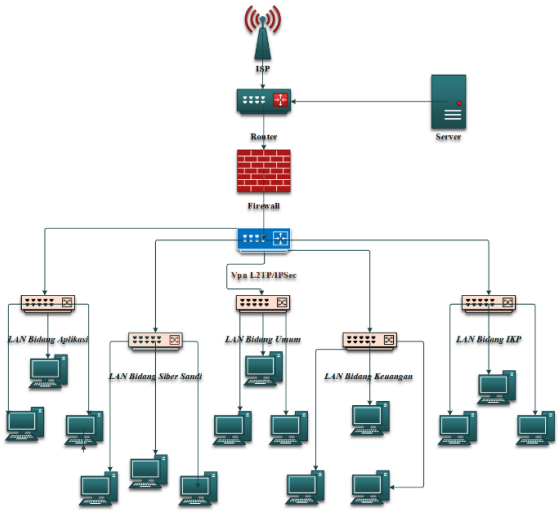
Implementasi ini dilaksanakan untuk mengenali apakah simulasi dari jaringan bisa berjalan sukses tanpa *error* dengan perencanaan awal. Percobaan dicoba hanya pada satu komputer *sever* dan beberapa komputer *client* tujuan untuk mengenali apakah rancangan cocok dengan perencanaan awal.

2.5. Pengujian

Pengujian dilakukan pada sistem keamanan jaringan tahap akhir dalam melakukan testing, guna untuk mengetahui kesalahan dalam penerepan. Pengujian dilakukan dengan melihat apakah sistem tersebut sudah berjalan dengan benar dan sesuai dengan perancangan yang dilakukan.

3. Hasil dan Pembahasan

Melakukan perancangan desain topologi yang dibuat dengan gambaran perancangan topologi *tree* yang dapat dilihat pada gambar 2 dibawah ini. Pada gambar 2 terdapat 4 macam perangkat jaringan yang digunakan yaitu, *ISP (Internet Service Provider)* sebagai modem, *router,* dan *switch*. Fungsi dari *router* dijadikan sebagai *mikrotik OS* yang menjadi gateway pada jaringan dan akses lalu lintas informasi data yang bertukar melalui jaringan internet dengan *mikrotik OS* yang sudah dikonfigurasi dengan *VPN (Virtual Private Network)* metode *L2TP (Layer 2 Tunneling Protocol)* dan *IPSec (IP Security)* agar lalu lintas tidak dapat ditemukan oleh pihak lain dalam satu jaringan yang sama.



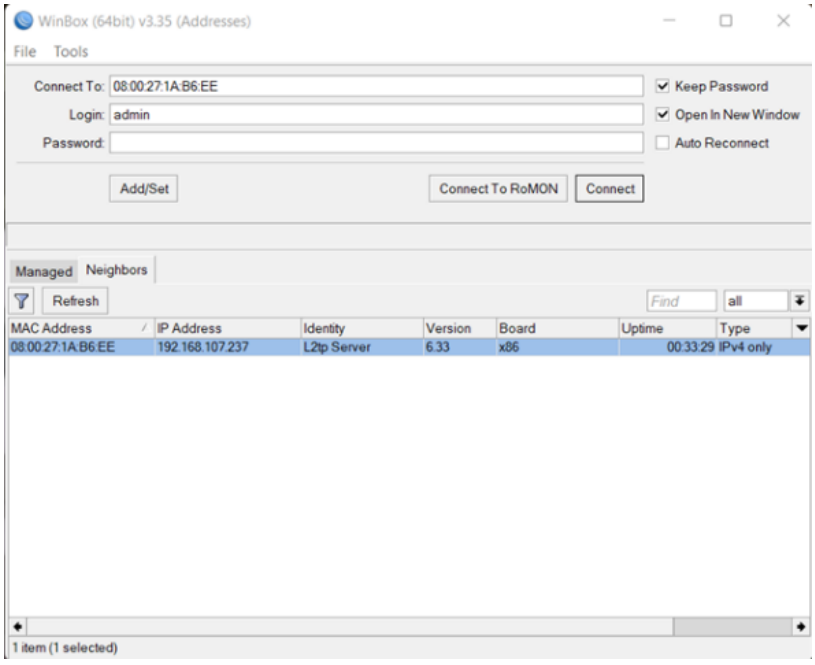
Gambar 2 Topologi Jaringan

Pada penelitan ini dilakukan perancangan pada sistem keamanan jaringan dengan menggunakan metode *L2TP (Layer 2 Tunneling Protocol)* dan *IPSec (IP Security)* sebagai alternatif keamanan jaringan berfungsi untuk mengidentifikasi dan mengevaluasi setiap permasalahan yang terjadi pada sistem keamanan jaringan.

3.1. Aplikasi Winbox

Penulis melakukan penginstalan aplikasi *Winbox* yang akan digunakan sebagai alat untuk konfigurasi keamanan jaringan. Adapun Langkah-langkah konfigurasi sebagai berikut:

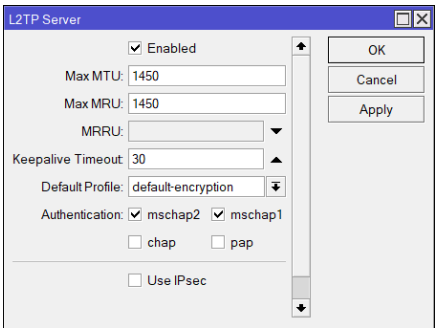
- Login Winbox



Gambar 3 Login Winbox

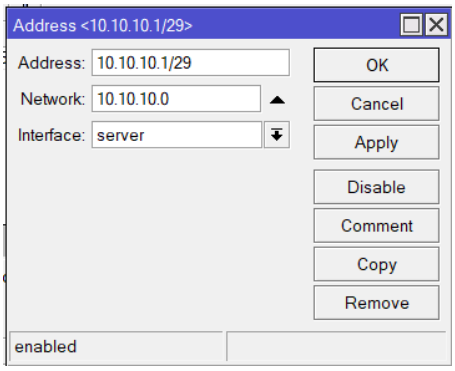
- Konfigurasi *IP Address*

Jurnal Sarjana Teknik Informatika
Vol. 10., No. 3, Oktober 2022, pp. 162-171

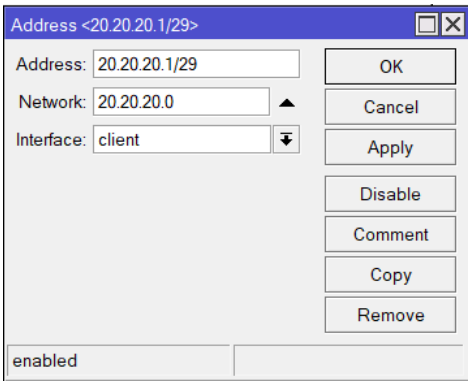


Gambar 4 *Setting IP Address Wlan*

Ethernet 1 merupakan *port* pertama yang digunakan untuk *wlan* yang berfungsi sebagai *Gateway* ntuk penghubung ke internet.



Gambar 5 *Setting IP Address Lokal (server)*

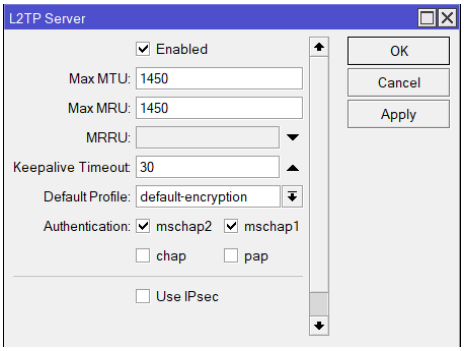


Gambar 6 *Setting IP Address Lokal (client)*

Ethernet 2 dan *Ether 3* merupakan *port* kedua yang digunakan untuk lokal yang berfungsi sebagai *Gateway* untuk penghubung ke PC.

- Menetapkan *L2TP*

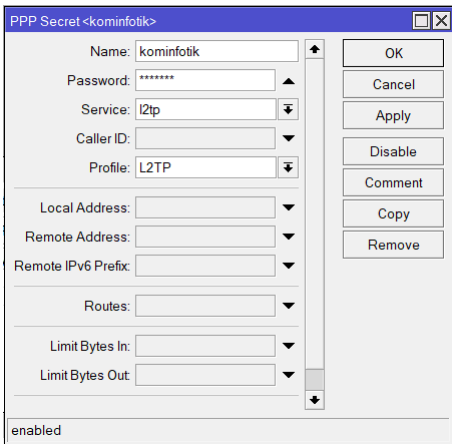
L2TP server merupakan pengembangan dari *PPTP* ditambah *L2F*. *L2TP* lebih *firewall freindly* dibandingkan jenis *VPN* yang lainya seperti *PPTP*.



Gambar 7 *Setting L2TP*

- Menetapkan Secrets VPN L2TP

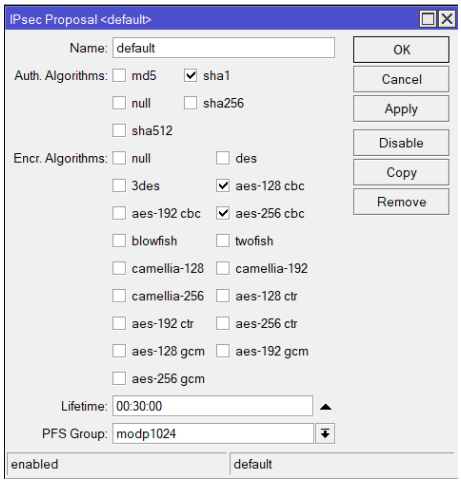
Mengisi beberapa parameter standar yang utama untuk melakukan koneksi. Seperti menentukan *username* dan *password* untuk proses autentikasi *client* yang akan terkoneksi ke *L2TP*.



Gambar 8 Konfigurasi *Secret L2TP*

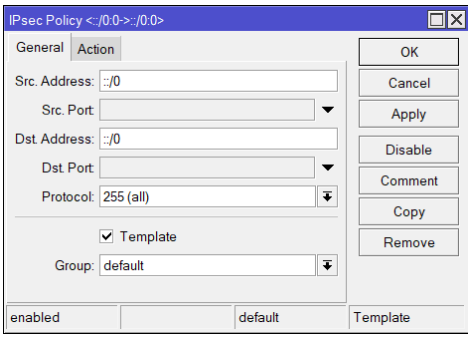
- Menetapkan *L2TP/IPSec*

Enskripsi pada *L2TP/IPSec* memiliki tingkat sekuritas lebih tinggi daripada *PPTP* yang mengunakan *MPPE*.

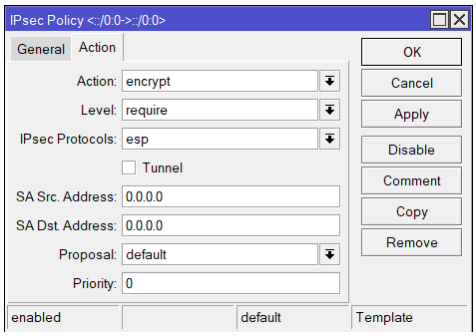


Gambar 9 Konfigurasi *L2TP/IPSec*

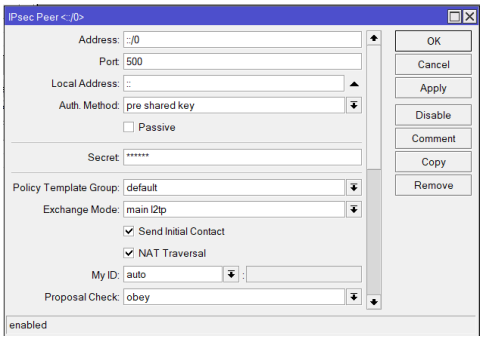
Jurnal Sarjana Teknik Informatika
Vol. 10., No. 3, Oktober 2022, pp. 162-171



Gambar 10 Konfigurasi *IPSec Policy*



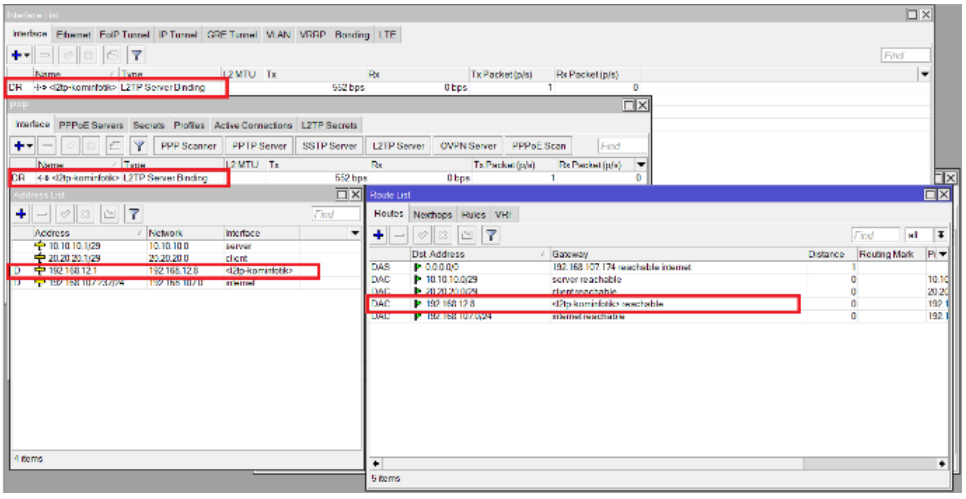
Gambar 11 Konfigurasi *Action IPSec Policy*



Gambar 12 Konfigurasi *IPSec Peer*

- Hasil Konfigurasi *L2TP dan IPSec*

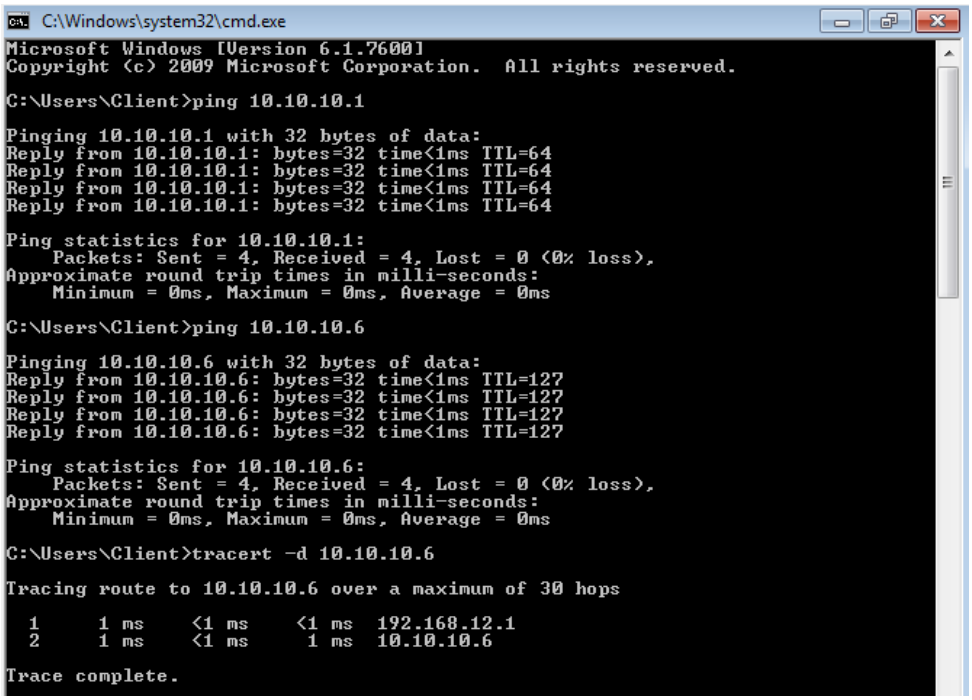
Dari hasil konfigurasi yang dilakukan diatas maka, secara otomatis *VPN L2TP* dan *IPSec* akan membuat *rule* sendiri menujukan bahwa hasil konfigurasi berhasil.



Gambar 13 Hasil *Konfigurasi L2TP/IPSec*

- *Dial* VPN Connection

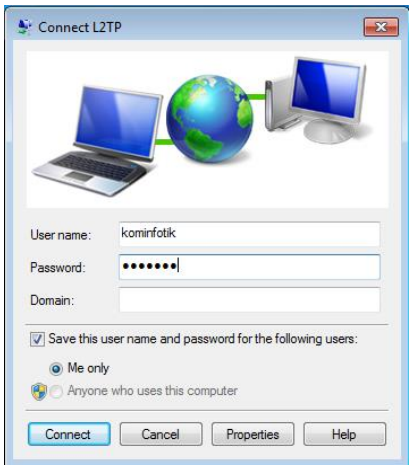
Hasil dari konfigurasi diatas dilakukan *testing* pada *cmd* dengan pengambilan data dilakukan pada saat *client* melakukan *dial VPN ke server*. Tujuan dari pengambilan data ini adalah melakukan pengamatan terhadap protokol *L2TP/IPsec* dalam membangun sebuah *tunnel VPN* sebelum informasi dapat di lewatkan melalui *tunnel* yang dibuat.



Gambar 14 *Dial VPN Connection*

3.2. *Login* Akun Jaringan *L2TP/IPSec*

Melakukan *login* akun yang telah dibuat pada *router server* sebelumnya guna untk terubung satu *(server)* dengan yang lain *(client)*.

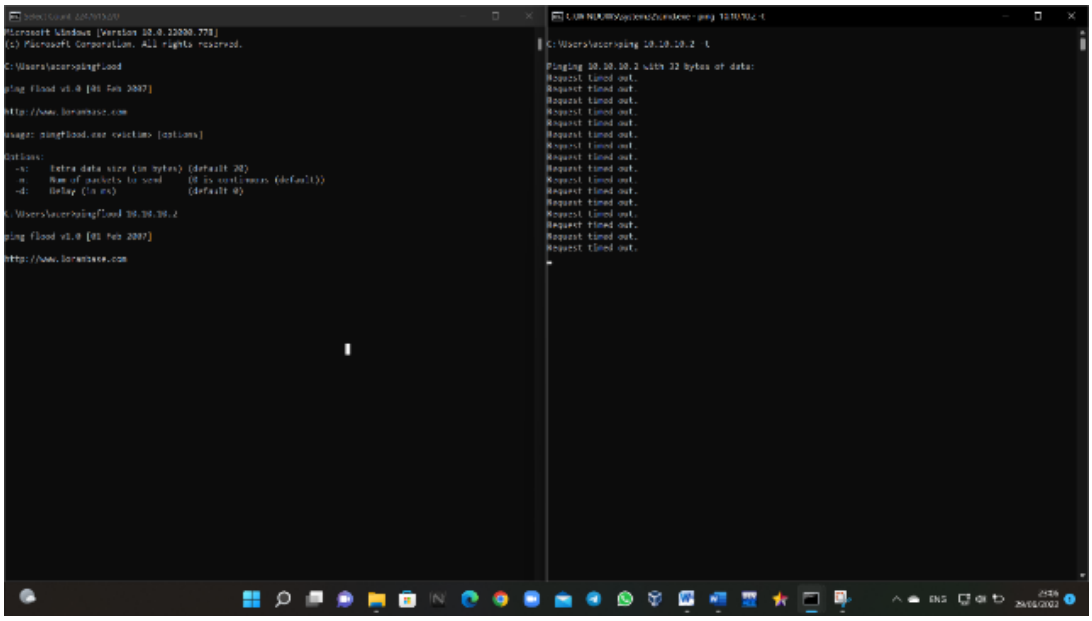


Gambar 15 *Dial Up Connect VPN L2TP/IPSec*

3.3. Pengujian Sistem

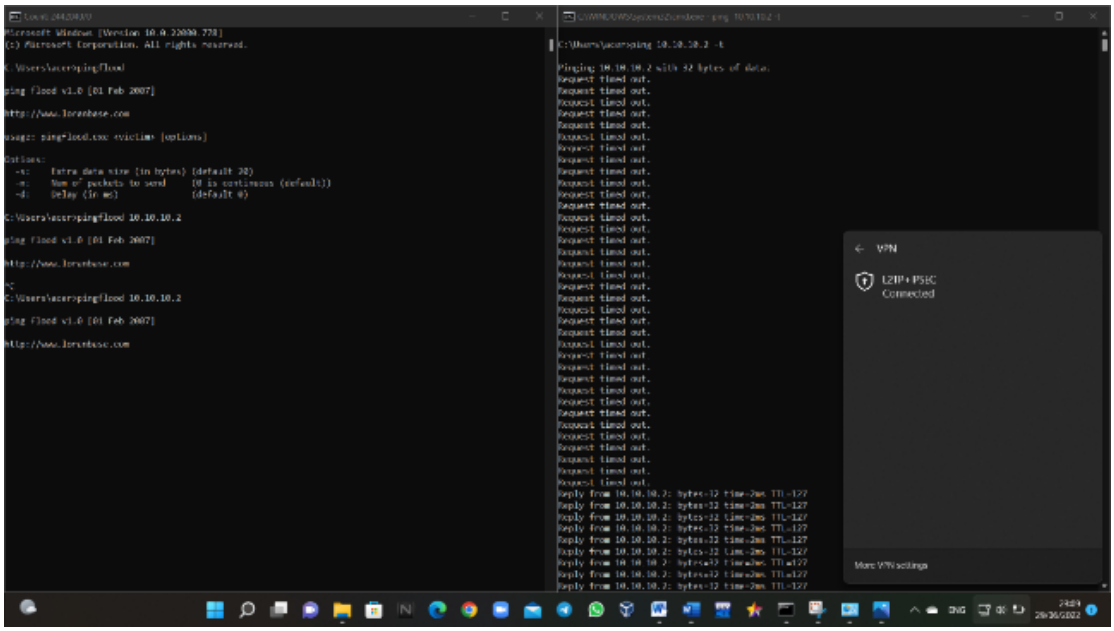
Pada tahapan pengujian ini akan dilakukan dengan mengunakan perintah ping pada cmd (command prompt) dengan penyerangan DDoS (Distributed Daniel of Service) menggunakan aplikasi pingflood.exe.

Jurnal Sarjana Teknik Informatika
Vol. 10., No. 3, Oktober 2022, pp. 162-171



Gambar 16 *DDOS Attack* tanpa *L2TP/IPSec*

Gambar 16 diatas menunjukkan hasil *Request Time Out (RTO).* Pengujian dilakukan dengan penyerangan *pingflood* menuju *ip address* dari *server* menunjukkan bahwa serangan berhasil dengan membuat *server* tidak merespon/menjawab yang berarti serangan berhasil membanjiri *traffic* jaringan *server.*



Gambar 17 *DDoS Attack* terhubung *L2TP/IPSec*

Gambar 17 diatas menunjukkan hasil ping berjalan. Pengujian dilakukan dengan penyerangan *pingflood* menuju *ip address* dari *server* menunjukkan bahwa serangan berhasil dialihkan oleh *VPN* protokol *L2TP* dan *IPSec* dengan membuat *server* tetap merespon yang berarti serangan berhasil mengatasi serangan walaupun *traffic* jaringan *server* sendang dibanjiri serangan oleh *DDoS Attack.*

4. Kesimpulan

Setelah menyelesaikan penelitan ini dapat diambil kesimpulan bahwa dengan melakukan konfigurasi *L2TP (Layer 2 Tunneling Protocol*) dan *IPSec (IP Security)* menggunakan aplikasi *winbox* dapat menghasilkan pengaturan keamanan pada *mikrotik* yang sudah dikonfigurasikan dan hasil konfigurasi dapat diterapkan.

Penggunaan protokol *L2TP (Layer 2 Tunneling Protocol)* dan *IPSec (IP Security)* sebagai alternatif keamanan jaringan menjadikan proses pertukaran data informasi menjadi terenkripsi oleh fitur keamanan yang terdapat pada *IPSec (IP Security)*. Hal ini dibuktikan dengan pengujian serangan *DDoS attack* yang menuju ke *IP Address* pada *server* yang mampu dialihkan oleh *L2TP (Layer 2 Tunneling Protocol)* dan *IPSec (IP Security)* dalam mengatasi serangan sehingga *server* tidak mudah *down*.

Daftar Pustaka

[1] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, "Perancangan Dan Implementasi Vpn Server Dengan Menggunakan Protokol Sstp (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 11, no. 1, 2017, doi: 10.35793/jti.11.1.2017.16745.

[2] P. Sihombing and W. Ginting, "Perancangan dan Implementasi Enkripsi dan Dekripsi File dengan Algoritma RC4 â€" One Time Pad pada Jaringan LAN," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 02, no. 01, pp. 1–10, 2020, doi: 10.54367/kakifikom.v2i1.663.

[3] A. Heryana and Y. M. Putra, "Perancangan Dan Implementasi Infrastruktur Jaringan Komputer Serta Cloud Strorage Server Berbasis Kendali Jarak Jauh (Studi Kasus Di Pt. Lapi Itb)," *Teknol. Inf. dan Komun.*, vol. IX, no. Cloud Storage, p. 7, 2018, [Online]. Available: http://jurnal.unnur.ac.id/index.php/jurnalfiki.

[4] D. Bayu Rendro and W. Nugroho Aji, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 2, pp. 108–115, 2020, [Online]. Available: https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/2522.

[5] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, 'Keamanan Jaringan Komputer Pada Era Big Data,' J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[6] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

[7] M. Ayub, A. Maulana, and A. Fauzi, "Penerapan Firewall Dan Protokol IpSec / L2TP Sebagai Solusi Keamanan Akses Jaringan Publik," vol. 1, no. 2, pp. 81–90, 2021.

[8] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta," *J. Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.

[9] B. Sutara, "Layanan Jaringan Internet Pada Virtual Private Network (VPN) Menggunakan L2TP Untuk Peningkatan Keamanan Jaringan," vol. 16, no. 1, pp. 1–6, 2017.

[10] F. Sjafrina, "Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional," *Proc. Semin. Nas. Teknol. Inf. dan Komun. STI&K (SeNTIK 2019)*, vol. 3, pp. 211–217, 2019.

[11] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 3, no. 2, pp. 260–267, 2018.

[12] Rudol, "Implementasi Keamanan Jaringan Komputer Pada Virtual Private Network (Vpn) Menggungakan," *Implementasi Keamanan Jar. Komput. Pada Virtual Priv. Netw. Menggungakan Ipsec*, vol. 2, no. 1, pp. 65–68, 2017.

[13] A. Micro, "Dibaca ,, Dipahami ,, Dicoba ,, Dievaluasi ,,,,, Jika masih ada kesalahan atau kegagalan , ulangi dibaca lagi … ~ Andi Micro ~," 2012.

[14] H. Kuswanto, "Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP," *Paradigma*, vol. 19, no. 1, pp. 46–51, 2017.

[15] L. D. Samsumar and S. Hadi, "PENGEMBANGAN JARINGAN KOMPUTER NIRKABEL (WiFi) MENGGUNAKAN MIKROTIK ROUTER (STUDI KASUS PADA SMA PGRI AIKMEL)," *Method. J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 1, pp. 1–9, 2018, doi: 10.46880/mtk.v4i1.59.