Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Implementasi Keamanan Data Pada Jaringan Router MikroTik Menggunakan VPN L2TP Dan IPSec

Implementation Of Data Security On MikroTik Router Network Using L2TP VPN And IPSec

Herjuno Dwi Nugroho[1], Yudi Sutanto[2]
[1,2] Informatika, Universitas AMIKOM Yogyakarta
*Email : [1]herjuno.nugroho@students.amikom.ac.id,[2]yudisuta@amikom.ac.id

ABSTRACT

The development of internet network technology provides convenience in communication and data exchange, but also increases the risk of information leakage. One solution to overcome this threat is the use of a Virtual Private Network (VPN). This study aims to implement and analyze the effectiveness of L2TP/IPSec VPN on MikroTik routers in dealing with sniffing and man-in-the-middle (MITM) attacks, as well as evaluate its impact on network service quality. The research method uses the Network Development Life Cycle (NDLC) approach which includes the stages of analysis, design, implementation, and testing. The results show that L2TP/IPSec VPN is able to protect data well from attacks because all traffic is encrypted. In terms of service quality, there is a decrease in throughput, latency, and jitter due to encryption, but the packet loss rate remains 0%, so the network remains stable. This study contributes by providing a reference for L2TP/IPSec VPN implementation on MikroTik, offering an efficient solution for data protection, and becoming a reference for further research in the field of network security.

Keywords : Network security, MikroTik, Virtual Private Network (VPN), L2TP, IPSec.

ABSTRAK

Perkembangan teknologi jaringan internet memberikan kemudahan dalam komunikasi dan pertukaran data, namun juga meningkatkan risiko kebocoran informasi. Salah satu solusi untuk mengatasi ancaman tersebut adalah penggunaan Virtual Private Network (VPN). Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis efektivitas VPN L2TP/IPSec pada router MikroTik dalam menghadapi serangan sniffing dan man-in-the-middle (MITM), serta mengevaluasi dampaknya terhadap kualitas layanan jaringan. Metode penelitian menggunakan pendekatan *Network Development Life Cycle* (NDLC) yang mencakup tahapan analisis, perancangan, implementasi, dan pengujian. Hasil penelitian menunjukkan bahwa VPN L2TP/IPSec mampu melindungi data dengan baik dari serangan karena seluruh lalu lintas terenkripsi. Dari sisi kualitas layanan, terjadi penurunan throughput, latency, dan jitter akibat enkripsi, tetapi tingkat *packet loss* tetap 0%, sehingga jaringan tetap stabil. Penelitian ini berkontribusi dengan memberikan referensi implementasi VPN L2TP/IPSec pada MikroTik, menawarkan solusi efisien untuk perlindungan data, serta menjadi acuan bagi riset lanjutan di bidang keamanan jaringan.

Kata kunci: Keamanan jaringan, MikroTik, Virtual Private Network (VPN), L2TP, IPSec.

I. PENDAHULUAN

Perkembangan teknologi saat ini berkembang sangat pesat terutama teknologi jaringan internet. Internet menjadi kebutuhan utama dalam komunikasi modern, memungkinkan transfer informasi dengan cepat dan efisien. Tidak hanya digunakan oleh individu, jaringan internet juga digunakan organisasi untuk bertukar informasi maupun mengirimkan data penting. Namun, meskipun memiliki banyak keunggulan, internet tidak menjamin pertukaran data tersebut aman. Banyak pihak yang tidak bertanggung jawab memanfaatkan celah keamanan internet mengakibatkan terjadinya kebocoran data, pencurian informasi, hingga kerugian finansial yang besar.

Seringnya aksi pencurian data menimbulkan kebutuhan akan solusi keamanan yang tepat. Salah satu metode yang efektif melindungi keamanan data adalah dengan menerapkan *Virtual Private Network* (VPN). VPN adalah sebuah koneksi *virtual* bersifat privat yang digunakan untuk mengenkripsi lalu lintas data sehingga tidak dapat diakses oleh pihak yang tidak berwenang [1]. Dari berbagai protokol VPN, *Layer 2 Tunneling Protocol* (L2TP) yang dikombinasikan dengan *Internet Protocol Security*

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

(IPSec) akan meningkatkan keamanan data dengan memberikan autentikasi dan enkripsi berlapis.

Sejumlah penelitian sebelumnya tentang VPN L2TP/IPSec lebih banyak berfokus pada aspek keamanan dari satu serangan [2] [3] [4], konektivitas antar-cabang [5] [6], atau perbandingan antarprotokol VPN [7] [8]. Namun, kajian yang secara khusus menyoroti implementasi VPN L2TP/IPSec pada MikroTik untuk jaringan skala kecil (SOHO) sekaligus mengevaluasi dampaknya terhadap *Quality of Service* (QoS) masih jarang dilakukan. Berdasarkan hal tersebut, penelitian ini bertujuan untuk mengkaji implementasi dan menguji keamanan VPN L2TP/IPSec pada *router* MikroTik dalam menghadapi serangan sniffing dan MITM, serta menganalisis dampak terhadap *Quality of Service* jaringan skala kecil hingga menegah (SOHO – *Small Office/Home Office*). Dengan demikian, diharapkan penelitian ini memberikan kontribusi dalam meningkatkan keamanan data individu maupun organisasi.

II. LANDASAN TEORI

A. Kajian Penelitian Terdahulu

Wicaksana (2023) merancang VPN L2TP/IPSec dari *server* ke komputer *client* untuk menangkal serangan DDoS menggunakan *pingflood.exe* dan terbukti berhasil meningkatkan keamanan sistem jaringan melalui enkripsi data yang dikirimkan [2]. Namun, penelitian ini terbatas pada jenis serangan DdoS saja, sedangkan ancaman lain seperti *sniffing* dan *Man-in-the-Middle* (MITM) belum diuji. Penelitian ini hadir untuk melengkapi dengan menguji efektivitas VPN L2TP/IPSec terhadap serangan tersebut.

Putra dkk. (2023) mengimplementasikan VPN tunnel berbasis MikroTik untuk mengamankan data dari serangan *sniffing* yang hasilnya lalu lintas tidak terlihat oleh penyusup [3]. Meski efektif terhadap sniffing, penelitian tersebut tidak menguji serangan MITM. Penelitian ini memperluas kajian dengan menguji kedua jenis serangan sekaligus.

Auliafitri dkk. (2024) menunjukkan bahwa MITM mampu mengakses data rahasia dari pengguna yang terhubung dalam jaringan menggunakan Websploit [4]. Penelitian tersebut membuktikan ancaman, tetapi tidak menawarkan solusi teknis. Penelitian ini berkontribusi dengan menguji VPN L2TP/IPSec sebagai solusi praktis untuk menghadapi MITM.

Taufiqurrochman dkk. (2023) menerapkan VPN L2TP/IPSec pada PT. Megacom untuk menghubungkan antar kantor dengan hasil koneksi berjalan dengan aman dan cepat melalui *tunneling* [5]. Fokus penelitian tersebut lebih pada konektivitas antar lokasi skala perusahaan, bukan pada pengujian serangan maupun evaluasi *Quality of Service* (QoS). Penelitian ini berbeda karena menguji VPN L2TP/IPSec pada jaringan skala kecil (SOHO) dengan simulasi serangan dan analisis QoS.

Penelitian lain oleh Pratama dkk. (2021) menggabungkan L2TP/IPSec dengan *port forwarding* pada MikroTik VPS untuk kemudahan monitoring jaringan secara *realtime* [6]. Meski inovatif, penelitian tersebut tidak menyoroti aspek ketahanan VPN terhadap serangan keamanan. Oleh karena itu, penelitian ini melengkapi celah tersebut dengan fokus pada keamanan dan QoS.

Pamungkas dkk. (2021) membandingkan PPTP dan L2TP/IPSec. Hasilnya L2TP/IPSec terbukti lebih unggul dalam aspek keamanan dan QoS [7]. Namun, penelitian tersebut sebatas pada perbandingan protokol tanpa adanya simulasi serangan. Penelitian ini melanjutkan dengan pendekatan pengujian keamanan langsung menggunakan sniffing dan MITM.

Fitrian dkk. (2025) membandingkan protokol VPN seperti PPTP, L2TP/IPSec, dan OpenVPN, serta pemanfaatan terknologi SD-WAN dan MPLS. Hasilnya PPTP menawarkan kecepatan tinggi, tingkat keamanannya tergolong rendah. L2TP/IPSec memliki keamanan yang lebih baik dengan adanya penurunan performa latency, sedangkan OpenVPN menawarkan keamanan yang lebih kuat, namun memerlukan sumber daya sistem yang lebih besar [8]. Walaupun memberikan gambaran komparatif yang luas, penelitian itu lebih fokus pada performa protokol dan kebutuhan sumber daya. Penelitian ini melengkapi dengan implementasi L2TP/IPSec pada MikroTik di jaringan SOHO, disertai pengujian terhadap ancaman serangan dan dampaknya terhadap QoS.

B. Dasar Teori

1. Jaringan Komputer

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Merupakan sekumpulan perangkat komputer yang terkoneksi melalui media kabel maupun nirkabel. Koneksi ini memungkinkan interaksi antar perangkat dengan protokol, tertentu untuk saling bertukar informasi, data, program hingga menggunakan perangkat keras secara bersama. melalui jaringan ini, data yang dikirimkan dapat mencakup format gambar, teks, video, maupun audio [9].

2. Keamanan Jaringan

Merupakan tindakan yang dilakukan untuk keamanan jaringan komputer dari potensi ancaman serangan yang merugikan. Definisi jaringan yang bukan hanya perangkat keras seperti *router*, *switch* dan *server*, namun mencakup perangkat lunak seperti *firewal* dan *antivirus* yang ada dalam jaringan [10].

3. *Open System Interconnection* (OSI)

Merupakan standar komunikasi jaringan yang dikembangkan oleh *International Standars Organization* (OSI), terdiri dari tujuh lapisan berurutan, masing-masing dengan fungsi spesifik untuk memfasilitasi pertukaran data antar perangkat. Lapisan tersebut meliputi *physical layer, data link layer, network layer, transport layer, session layer, presentation layer,* dan *application layer* [11].

4. MikroTik

Merupakan dan perangkat keras yang digunakan untuk membangun jaringan komputer dengan sistem operasi MikroTik RouterOS [12]. MikroTik RB951Ui-2HnD cocok digunakan pada jaringan skala kecil hingga menengah karena dilengkapi RouterOS dengan fitur manajemen jaringan lengkap, termasuk dukungan berbagai protokol VPN (PPPoE, PPTP, L2TP/IPSec, SSTP, OpenVPN). Perangkat ini memiliki 5 port *Ethernet*, *port USB* untuk modem 3G/4G, fitur *PoE-out*, serta *wireless* 2.4GHz *dual chain*. Namun, keterbatasan *processor* membuatnya kurang optimal untuk jaringan dengan *traffic* tinggi, dan belum mendukung *WiFi* 5GHz [13].

5. *Development Life Cycle* (NDLC)

Merupakan metode terstruktur untuk merancang sistem jaringan komputer melalui enam tahapan, yaitu *analysis, design, simulation/prototype, implementation, monitoring,* dan *management*. NDLC bergantung proses pengembangan sebelumnya seperti perencanaan strategi, pengembangan aplikasi, dan analisis distribusi data, sehingga menghasilkan sistem jaringan yang akurat dan sistematis [14].

6. VPN L2TP/IPSec

Virtual Private Network (VPN) adalah layanan yang memungkinkan koneksi privat ke jaringan lain melalui internet, awalnya digunakan untuk melindungi data sensitif perusahaan. Saat ini, VPN banyak digunakan untuk mengakses konten terbatas [12]. *Layer 2 Tunneling Protocol* (L2TP) merupakan jenis *VPN* yang menyediakan terowongan aman yang dikombinasi dengan *IPSec* dengan mengaktifkan *port* 1701 [15]. *Internet Protocol Security* (IPSec) merupakan protokol yang menjamin keamanan data dengan menyediakan enkripsi, autentikasi, dan integritas data guna mencegah peretasan dan manipulasi [10].

7. *Sniffing*

Merupakan metode penyadapan lalu lintas jaringan dengan memanfaatkan mode *promiscuous* pada *ethernet*. Teknik ini digunakan untuk menganalisis data biner dalam jaringan oleh administrator untuk pemantauan jaringan maupun oleh penyerang untuk mencuri data. Pencegahan efektif terhadap *sniffing* adalah dengan mengenkripsi komunikasi menggunakan protokol seperti SSH, SSL, atau SecureFTP [16].

8. *Man-in-the-Middle Attack*

Merupakan serangan cara penyerang menyusup di antara dua pihak yang berkomunikasi untuk memantau atau memanipulasi data yang dikirimkan keduanya. Contohnya, penyerang membajak koneksi *Wi-Fi* publik guna mencuri informasi rahasia seperti kata sandi atau data kartu kredit, hingga memanipulasi data komunikasi untuk mendapatkan akses masuk ke sistem [17].

9. *Quality of Service*

Merupakan standar untuk menilai kualitas layanan jaringan berdasarkan pengalaman pengguna akhir. Tujuannya adalah memastikan jaringan mampu mengirim data secara andal guna menjaga kepuasan

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

pengguna. Parameter pengukuran QoS mengacu pada standar TIPHON dan ITU-T. Parameter meliputi *throughput, bandwidth, delay, jitter,* dan *packet loss* [18].

III. METODE PENELITIAN

A. Objek Penelitian

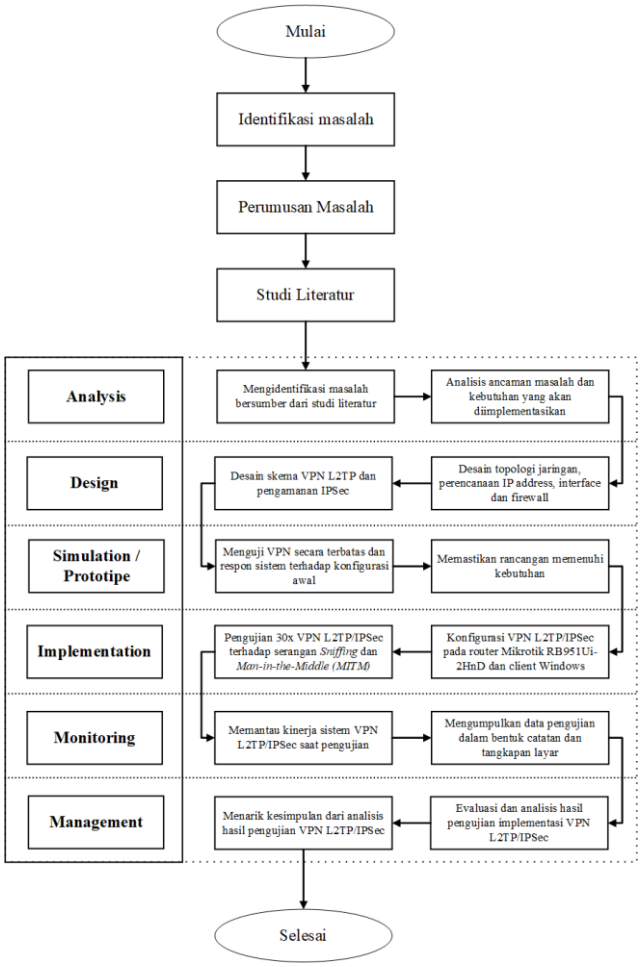
Objek penelitian akan berfokus pada jaringan komputer dengan perangkat utama berupa *router* MikroTik RB951Ui-2HnD mengimplementasikan VPN L2TP/IPSec. Protokol L2TP digunakan untuk membuat terowongan komunikasi data antar jaringan, sementara IPSec berperan dalam melakukan enkripsi dan autentikasi data yang ditransmisikan.

Penelitian ini menargetkan penerapan teknologi VPN dalam konteks peningkatan keamanan data yang ditransmisikan terhadap ancaman keamanan, khususnya serangan *Sniffing* dan *Man-in-the-Middle attack* (MITM). Selain itu mencakup evaluasi dampak implementasi VPN terhadap *Quality of Service*, yang dinilai berdasarkan parameter *throughput, packet loss, latency,* dan *jitter*.

Penelitian dilaksanakan mulai dari bulan Januari hingga Juni 2025. Lokasi penelitian berada di Sanjuro Komputer, yang merupakan rumah pribadi peneliti dan telah disesuaikan telah disesuaikan jaringan skala kecil hingga menengah (SOHO - *Small Office/Home Office*).

B. Alur Penelitian

Penelitian akan menggunakan metode *Network Development Life Cycle* (NDLC). Objek penelitian akan berfokus pada jaringan komputer dengan perangkat utama berupa *router* MikroTik RB951Ui-2HnD yang mengimplementasikan VPN L2TP/IPSec.

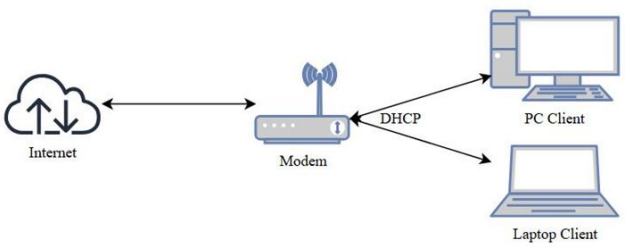


Gambar 1 Alur Penelitian Metode NDLC

Tahapan dalam alur penelitian adalah sebagai berikut:

1. Analysis

Identifikasi masalah keamanan jaringan berbasis MikroTik yang bersumber studi literatur berupa jurnal. Analisis difokuskan pada resiko jaringan tanpa VPN dan kebutuhan sistem keamanan dengan VPN L2TP/IPSec

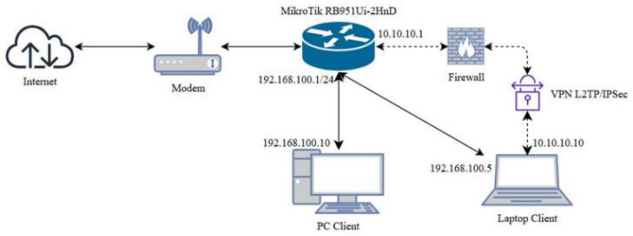


Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Gambar 2 Topologi Jaringan Lama

2. Design

Merancang jaringan sesuai kebutuhan dari hasil analisis sebelumnya meliputi topologi jaringan, rencana *IP Address*, konfigurasi *interface* dan *firewall*, dan desain skema VPN L2TP/IPSec.



Gambar 3 Desain Topologi Jaringan Baru

Tabel 1 Konfigurasi IP Address

Perangkat	IP Address	Default Gateway
MikroTik	192.168.100.1/28	
MikroTik VPN	10.10.10.1/24	
Client Windows 10	192.168.100.5 /28	192.168.100.1
VM Windows 7	192.168.100.10 /28	192.168.100.1
VM Kali Linux	192.168.100.14 /28	192.168.100.1
VPN Client 1	10.10.10.10/24	10.10.10.1
VPN Client 2	10.10.10.20/24	10.10.10.1

3. Simulation / Prototipe

Melakukan simulasi awal untuk memastikan rancangan VPN L2TP/IPSec berjalan sesuai fungsi dan memenuhi aspek keamanan dasar.

4. Implementation

Implementasi desain dengan mengaktifkan L2TP *Server* dan IPSec pada perangkat MikroTik RB951Ui-2HnD serta konfigurasi VPN *client* pada klien Windows. pengujian dilakukan dengan simulasi serangan Sniffing dan MITM sebanyak 30 kali.

5. Monitoring

Mengawasi kinerja sistem dan mengumpulkan data penelitian meliputi hasil simulasi serangan *sniffing* dan MITM menggunakan aplikasi Ettercap, serta tangkapan paket lalu lintas jaringan menggunakan Wireshark. Selain itu, dilakukan juga pengukuran *Quality of Service* menggunakan iPerf3 yang mencakup parameter seperti *throughput, packet loss, latency* dan *jitter*. Seluruh hasil pengujian didokumentasikan dalam bentuk catatan dan tangkapan layar *(screenshot)*.

6. Management

Melakukan analisis dan evaluasi untuk menilai efektivitas sistem yang telah diimplementasikan. Analisis data dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah VPN L2TP/IPSec. Evaluasi difokuskan pada efektivitas VPN terhadap serangan serta dampaknya pada QoS.

C. Alat dan Bahan

Penelitian ini membutuhkan alat dana bahan guna menunjang proses penelitian, berikut kebutuhan perangkat keras dan perangkat lunak:

1. Perangkat Keras
   a. MikroTik RB951Ui-2HnD sebagai objek utama penelitian. Perangkat ini akan diimplementasikan VPN L2TP/IPSec untuk peningkatan keamanan data yang ditransmisikan terhadap ancaman keamanan.

Tabel 2 Spesifikasi MikroTik RB951Ui-2HnD

Spesifikasi Perangkat	
CPU	AR9344 single core 600mHz
RAM	128MB
Storage	128MB NAND
Port	5
Wireless	802.11b/g/n
OS	RouterOS license level 4

   b. Laptop Acer Swift 3 SF314-56G untuk mengkonfigurasi *router* MikroTik dan akan melakukan percobaan serangan terhadap sistem keamanan yang telah diimplementasikan pada *router*.

Tabel 3 Spesifikasi Laptop Acer Swift 3

Spesifikasi Perangkat	
Processor	Intel Core i5-8265U
Memory	12GB DDR4
Storage	SSD 256GB & HDD 1TB
GPU	Intel UHD 620 & Nvidia MX250

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Networking	Wi-Fi 802.11ac Dual Band (2.4 GHz and 5 GHz) 2x2 MU-MIMO technology
OS	Windows 10 Home

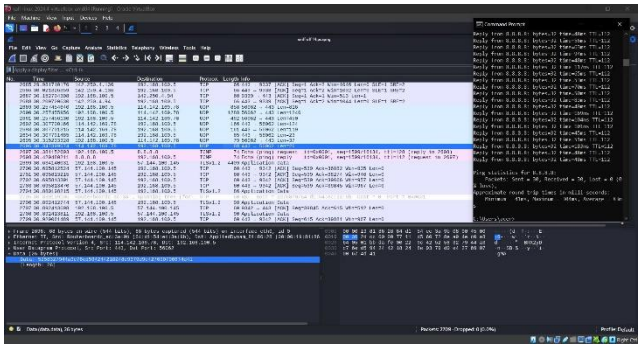
c. Kabel UTP Cat5e digunakan untuk menghubungkan *router* MikroTik dengan laptop konfigurasi.

2. Perangkat Lunak
   a. Windows 10 sebagai sistem operasi untuk konfigurasi sistem keamanan dan klien VPN.
   b. Windows 7 sebagai sistem operasi untuk klien pengujian *Quality of Service*.
   c. Winbox sebagai *software* yang digunakan untuk konfigurasi MikroTik.
   d. Oracle VM VirtualBox sebagai *software* virtualisasi untuk menginstal Kali Linux dalam Windows
   e. Kali Linux sebagai sistem operasi untuk pengujian serangan
   f. Wireshark sebagai *tools* yang digunakan untuk serangan *Sniffing*.
   g. EtterCap sebagai *tools* yang digunakan untuk serangan *Man-in-the-Middle.*
   h. Iperf3 sebagai *tools* yang digunakan untuk pengujian *Quality of Service*.

IV. HASIL PENELITIAN DAN PEMBAHASAN

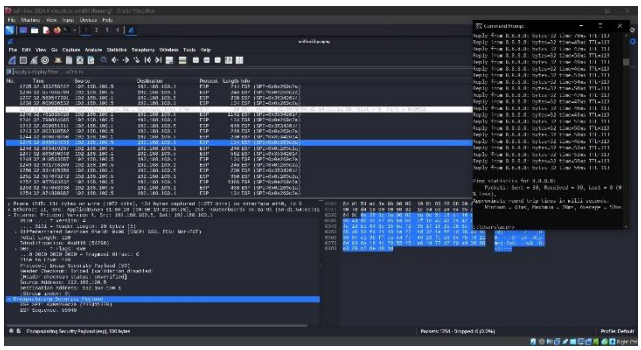
A. Hasil Pengujian Serangan *Sniffing*

Pengujian serangan *sniffing* dilakukan menggunakan Wireshark di Kali Linux (VM) mode *bridge* untuk memantau lalu lintas jaringan yang sama dengan klien Windows 10. Pengujian dilakukan 30 kali dalam kondisi VPN L2TP/IPSec aktif dan nonaktif, dengan aktivitas *ping* ke 8.8.8.8 sebagai simulasi lalu lintas jaringan.



Gambar 4 Pengujian Sniffing Saat VPN L2TP/IPSec Nonaktif

Hasilnya, saat VPN nonaktif, Wireshark menangkap berbagai paket data yang melintas. Banyak IP Address dan protokol yang muncul dalam tangkapan paket, termasuk paket ICMP (*ping*) ke 8.8.8.8 dapat dibaca secara jelas informasi waktu dan identitas setiap request-reply. Hal ini menunjukkan bahwa seluruh lalu lintas jaringan dapat disadap dengan mudah.



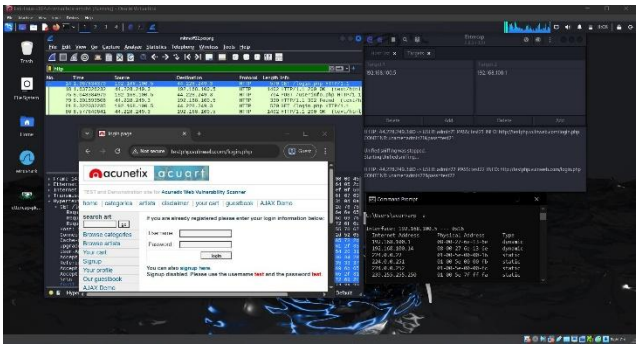
Gambar 5 Pengujian Sniffing Saat VPN L2TP/IPSec Aktif

Setelah VPN diaktifkan, lalu lintas jaringan terenkripsi menggunakan protokol ESP, termasuk aktivitas ping ke 8.8.8.8, isi data tidak terbaca dan tidak terlihat sebagai paket ICMP biasa. Namun, protokol layer 2 seperti ARP dan STP tetap terlihat karena tidak masuk dalam *tunnel* VPN. Temuan ini sejalan dengan penelitian Putra dkk. (2023) yang menunjukkan bahwa VPN dapat menyembunyikan lalu lintas data dari sniffing [3], sekaligus memperkuat bahwa penggunaan VPN L2TP/IPSec secara signifikan mengurangi potensi kebocoran data dengan mengarahkan lalu lintas melalui terowongan terenkripsi.

B. Hasil Pengujian Serangan *Man-in-the-Middle*

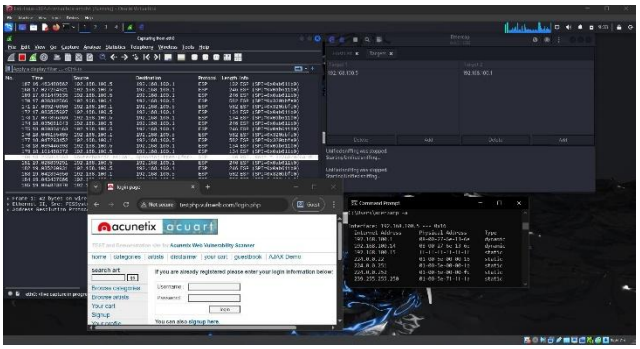
Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

Pengujian serangan *Man-in-the-Middle* (MITM) dilakukan menggunakan Ettercap di Kali Linux (VM) mode *bridge* dengan skenario *ARP spoofing* antara klien Windows 10 dan *router* MikroTik. Pengujian dilakukan 30 kali dalam kondisi VPN L2TP/IPSec aktif dan nonaktif, dengan aktivitas *login* HTTP ke situs uji coba *http://testphp.vulnweb.com/login.php* dengan berbagai kombinasi *username* dan *password* yang berbeda.



Gambar 6 Pengujian MITM Saat VPN L2TP/IPSec Nonaktif

Saat VPN L2TP/IPSec nonaktif, Ettercap berhasil melakukan *ARP spoofing* dan menangkap data login berupa *username* dan *password* yang dimasukkan klien saat aktivitas login sangat jelas karena lalu lintas jaringan tidak terenkripsi. Sama halnya dengan penelitian Auliafitri dkk. (2024) yang membuktikan bahwa serangan MITM menggunakan Websploit mampu mengakses data rahasia dari pengguna yang tidak dienkripsi [4]. Hasil ini menegaskan bahwa jaringan tanpa VPN memiliki kerentanan serius terhadap pencurian data melalui serangan MITM.

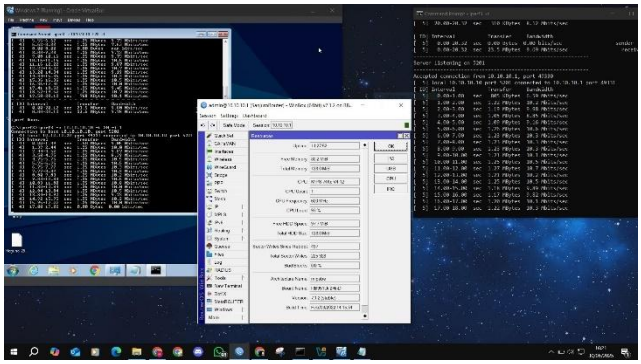


Gambar 7 Pengujian MITM Saat VPN L2TP/IPSec Aktif

Setelah VPN diaktifkan, *ARP spoofing* tetap berhasil, Namun, aktivitas login HTTP yang dilakukan klien Windows tidak berhasil terbaca. Semua paket telah terenkripsi menjadi protokol ESP oleh IPSec. Hasilnya Ettercap dan Wireshark hanya menangkap data yang sudah terenkripsi tanpa mendapatkan informasi *login* HTTP. Dengan demikian VPN L2TP/IPSec terbukti mampu mencegah kebocoran data dalam simulasi serangan MITM yang terjadi meskipun lalu lintas berhasil dialihkan ke penyerang.

C. Hasil Pengujian *Quality of Service*

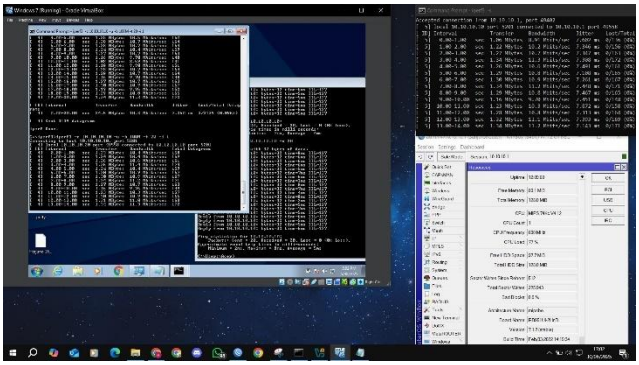
Pengujian *Quality of Service* dilakukan menggunakan Iperf3 dengan Windows 10 sebagai *server* dan Windows 7 (VM) sebagai *client*, keduanya terhubung ke *router* MikroTik RB951Ui-2HnD dalam jaringan 192.168.100.0/28. Saat VPN L2TP/IPSec aktif, masing-masing perangkat memperoleh *IP* 10.10.10.10 dan 10.10.10.20. Pengujian dilakukan sebanyak 30 kali pada kondisi *VPN* aktif dan nonaktif menggunakan protokol TCP *(throughput)* dan UDP *(latency* dan *jitter)*, dengan bandwidth 100 Mbps dan durasi 20 detik. Parameter yang diuji meliputi *throughput, packet loss, latency,* dan *jitter*.



Gambar 8 Pengujian Dengan Protokol TCP iPerf3

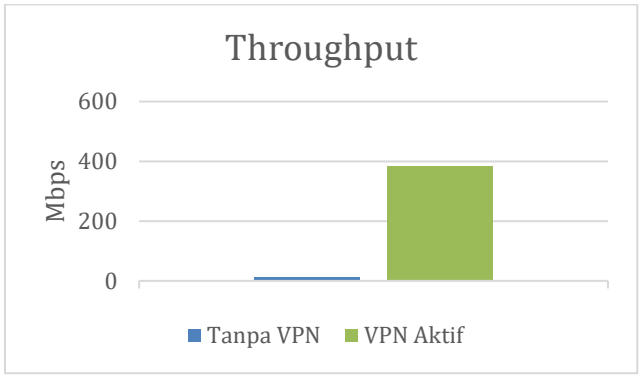
Tampilan pengujian throughput dengan protokol TCP di iPerf3, Windows 10 menjalankan perintah "iperf3.exe -s" untuk membuka sesi sebagai server iPerf3. Di sisi Windows 7 (client), perintah yang dijalankan adalah "iperf3 -c 10.10.10.10 -t 30 -i 1"

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

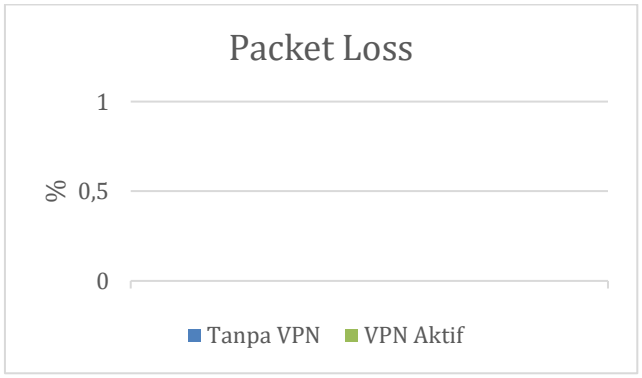


Gambar 9 Pengujian Dengan Protokol UDP iPerf3

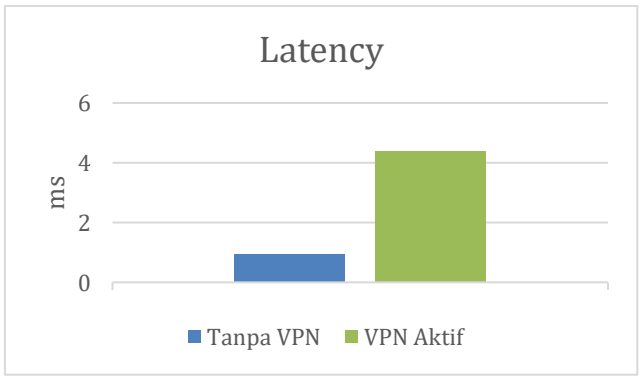
Tampilan pengujian latency dan jitter dengan protocol UDP di iPerf3, Di sisi Windows 7 (klien), perintah yang dijalankan adalah "iperf3.exe -c 10.10.10.10 -u -b 100M -t 20 -i 1" dan untuk pengujian packet loss klien melakukan ping ke IP windows 10.



Gambar 10 Diagram Batang Rata-Rata Throughtput



Gambar 11 Diagram Batang Rata-Rata Packet Loss

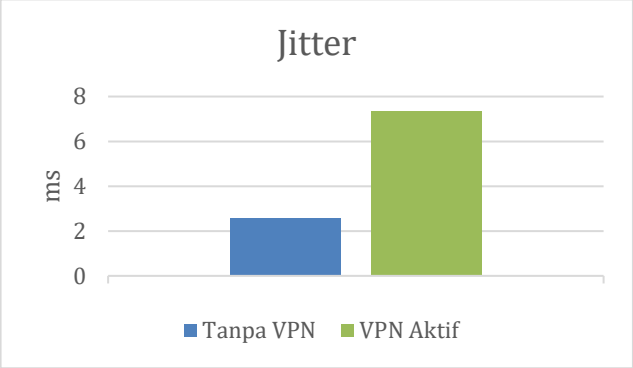


Gambar 12 Diagram Batang Rata-Rata Latency

Tabel 4 Perbandingan Rata-Rata Hasil Pengujian Quality of Service

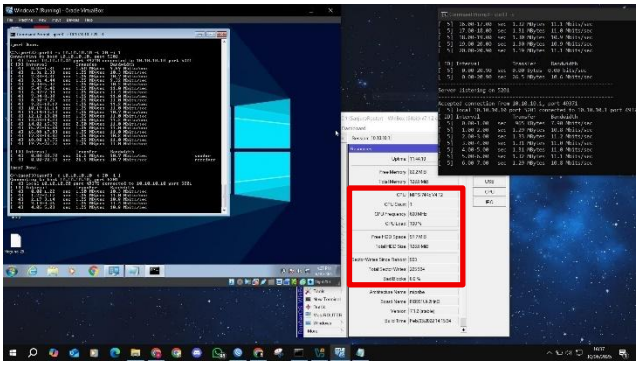
Parameter	**Tanpa VPN**	**VPN aktif**	**Keterangan**
Throughput (Gbits/s)	384,30	10,17	Turun drastis
Packet Loss (%)	0	0	Tidak berubah
Latency (ms)	0,93	4,40	Meningkat Signifikan
Jitter (ms)	2,55	7,34	Meningkat Signifikan

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373



Gambar 13 Diagram Batang Rata-Rata Jitter

Dari hasil pengujian, terjadi penurunan performa jaringan saat VPN aktif. Rata-rata *throughput* turun dari 384,30 Mbps menjadi 10,17 Mbps, *latency* meningkat signifikan dari 0,93 ms menjadi 4,4 ms, dan *jitter* naik dari 2,55 ms menjadi 7,34 ms. Namun, *packet loss* tetap 0% pada kedua kondisi. Temuan ini sejalan dengan penelitian Auliafitri (2025) yang juga mengungkap adanya *trade-off* antara keamanan dan performa pada protokol L2TP/IPSec. Semakin tinggi tingkat enkripsi yang diberikan untuk menjaga keamanan data, semakin besar pula membebani perangkat [8].



Gambar 14 Router MikroTik Saat Pengujian QoS

Penurunan performa jaringan terjadi karena beban kerja proses enkripsi dan autentikasi setiap paket data pada protokol IPSec dan keterbatasan performa *router* MikroTik RB951Ui-2HnD. Gambar 14 yang menunjukan load CPU mencapai 100% saat pengujian QoS dengan VPN aktif. Implikasinya, VPN L2TP/IPSec pada perangkat MikroTik berspesifikasi terbatas kurang cocok untuk jaringan dengan trafik tinggi, namun tetap efektif digunakan pada skala SOHO dengan kebutuhan moderat karena mampu menjaga keamanan data tanpa mengganggu stabilitas jaringan.

V. KESIMPULAN

A. Kesimpulan

Berdasarkan hasil pengujian implementasi VPN L2TP/IPSec pada router MikroTik RB951Ui-2HnD, maka didapatkan kesimpulan:

1. Implementasi VPN L2TP/IPSec pada *router* MikroTik RB951Ui-2HnD dapat dilakukan dengan mudah tanpa perangkat lunak maupun lisensi tambahan karena sudah memiliki fitur tersebut didalamnya.
2. VPN L2TP/IPSec efektif melindungi data dari serangan *Sniffing* dan *Man-in-the-Middle* (MITM) dengan enkripsi menggunakan protokol Encapsulating Security Payload (ESP).
3. Implementasi VPN L2TP/IPSec berdampak pada *Quality of Service* dengan penurunan performa jaringan, namun tetap menunjukkan stabilitas yang baik.
4. Solusi ini cocok untuk jaringan skala kecil hingga menengah (SOHO - *Small Office/Home Office*) namun kurang ideal untuk jaringan berskala besar atau *enterprise* yang menuntut kinerja lebih tinggi.
5. Penelitian ini memiliki keterbatasan pada skala pengujian yang sederhana dan penggunaan perangkat MikroTik RB951Ui-2HnD, sehingga hasilnya belum mencerminkan kondisi di jaringan dengan beban yang lebih kompleks

B. Saran

Berdasarkan hasil penelitian ini, maka disampaikan beberapa saran sebagai berikut:

1. Mengembangkan penelitian dengan topologi lebih kompleks, seperti *site-to-site* VPN, agar lebih mendekati skenario dunia nyata.
2. Menggunakan router dengan spesifikasi lebih tinggi untuk mengurangi beban CPU akibat proses enkripsi dan meningkatkan performa jaringan.
3. Menambahkan konfigurasi *firewall* dan *filter rules* untuk memperkuat keamanan jaringan.
4. Memperluas skenario pengujian dengan melibatkan berbagai jenis serangan selain *Sniffing* dan MITM, sehingga efektivitas VPN L2TP/IPSec dapat dievaluasi lebih menyeluruh.

Jurnal EEMISAS, Vol. 4, No. 1, Juni 2025, Hal. 35-45
Journal of Electrical, Electronic, Mechanical, Informatic and Social Applied Science
ISSN 2964-1373

REFERENSI

[1] M. A. Wardana, A. Z. Nusri, and J. Juliandika, "Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng," *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, vol. 5, no. 2, pp. 107–116, Oct. 2022, doi: 10.57093/jisti.v5i2.135.

[2] P. Wicaksana, "Implementasi VPN Server Menggunakan Protokol L2TP dan Metode IPSEC," *Jurnal Sains Informatika Terapan*, vol. 2, no. 3, pp. 119–123, Oct. 2023, doi: 10.62357/jsit.v2i3.204.

[3] R. E. Putra, N. Jalinusl, R. Islami, and M. Iqbal, "MENGAMANKAN SERANGAN PACKET SNIFFING PADA JARINGAN KOMPUTER MENGGUNAKAN VPN TUNNEL," *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 22, no. 2, p. 340, Aug. 2023, doi: 10.53513/jis.v22i2.7438.

[4] D. Auliafitri, E. RizkiSuro, M. R. M. Malik, and A. Setiawan, "Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit," *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 12, Jun. 2024, doi: 10.47134/pjise.v1i3.2620.

[5] T. Taufiqurrochman, S. Broto, and A. Armin, "PERANCANGAN JARINGAN VPN MENGGUNAKAN MIKROTIK DENGAN METODE L2TP/IPSEC," *JEIS: JURNAL ELEKTRO DAN INFORMATIKA SWADHARMA*, vol. 3, no. 2, pp. 29–41, Jul. 2023, doi: 10.56486/jeis.vol3no2.361.

[6] H. Pratama and N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP," *Creative Information Technology Journal*, vol. 7, no. 1, p. 51, Mar. 2021, doi: 10.24076/citec.2020v7i1.253.

[7] A. P. Pamungkas, Muhammad Reza Putra, and M. Hafizh, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-muko," *Jurnal KomtekInfo*, pp. 189–194, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.143.

[8] H. Pribadi Fitrian, A. Aulia Nurani, I. Mulhakim, N. Maesaroh, and P. Raharja, "ANALISIS MANAJEMEN TRAFIK JARINGAN PADA VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN PROTOKOL PPTP, L2TP/IPSEC, DAN OPEN VPN," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, pp. 2310–2314, Mar. 2025, doi: 10.36040/jati.v9i2.12926.

[9] Kustanto and D. T. Saputro, *Belajar Jaringan Komputer Berbasis MikroTik OS*, 1st ed. Yogyakarta: GAVA MEDIA, 2015.

[10] S. T. M. M. M. K. Agung Rachmat Raharja, *KEAMANAN JARINGAN*. PENERBIT KBM INDONESIA, 2024. [Online]. Available: https://books.google.co.id/books?id=kW0REQAAQBAJ

[11] M. K. Anggun Fergina, S. T. M. T. I. Dwi Sartika Simatupang, M. S. Dhita Diana Dewi, and S. P. M. M. Lusiana Sani Parwati, *Buku Ajar Jaringan Komputer dan Keamanan*. Kaizen Media Publishing, 2024. [Online]. Available: https://books.google.co.id/books?id=rOjvEAAAQBAJ

[12] A. A. Zackiansyah, M. R. GR, and A. S. R. C, *Easy and Practice PPPoE Server, VPN PPTP, Bandwidth Management, Mikrotik Hotspot with Mikrotik RouterBoard*. in Mikrotik Router. XP Solution Surabaya, 2022. [Online]. Available: https://books.google.co.id/books?id=XP18EAAAQBAJ

[13] E. A. Elazm, *MikroTik MTCNA*. CAN FOR LEARNING AND DEVE, 2025. [Online]. Available: https://books.google.co.id/books?id=ihc8EQAAQBAJ

[14] D. N. Amadi, A. Budiman, and P. Utomo, "Analysis of the effectiveness of VPN and PPTP Protocol in E-Link Health Report Application Using NDLC Method," *Journal of Information Systems and Informatics*,

vol. 6, no. 2, pp. 949–958, Jun. 2024, doi: 10.51519/journalisi.v6i2.746.

[15] D. Kuswanto, *Dasar Jaringan Komputer Windows Teori & Praktek*. Media Nusa Creative (MNC Publishing), 2022. [Online]. Available: https://books.google.co.id/books?id=sk2eEAAAQBAJ

[16] S. K. Muhammad Badriatul Anam, *Administrasi Sistem Jaringan SMK/MAK Kelas XII*. Gramedia Widiasarana indonesia, 2021. [Online]. Available: https://books.google.co.id/books?id=7vwWEAAAQBAJ

[17] S. K. M. S. Victor Benny Alexsius Pardosi *et al.*, *SISTEM KEAMANAN KOMPUTER*. CV Rey Media Grafika, 2024. [Online]. Available: https://books.google.co.id/books?id=wcD_EAAAQBAJ

[18] M. K. Aziel C. Nurcahyo, M. K. Listra Firgia, and S. S. M. K. Ag. Rudatyo Himanunanto, *KONFIGURASI & ANALISIS JARINGAN BERBASIS MIKROTIK*. AMERTA MEDIA, 2021. [Online]. Available: https://books.google.co.id/books?id=7HFrEAAAQBAJ