Prosiding-Seminar Nasional Teknologi Informasi & Ilmu Komputer ***(SEMASTER)***
Vol 4.No.1 2025 Hal 527-535

Analisis Serangan Man-In-The-Middle (Mitm) Dan Denial Of Service (Dos) Pada Protokol L2tp/Ipsec Berdasarkan Aspek Quality Of Service

Ahmad Safri Nasution[1], Wenni Syafitri[2]
[1,2]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning
[1,2]Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Riau, telp. 0811 753 2015
e-mail: [1]ahmad.safri.71@gmail.com, [2]wennisyafitri@unilak.ac.id

Abstrak

Penelitian ini mengevaluasi kinerja dan ketahanan keamanan protokol L2TP/IPsec terhadap serangan Man-in-the-Middle (MITM) dan Denial of Service (DoS) pada lingkungan jaringan PT. XYZ. Pengujian QoS mencatat throughput puluhan Mbps, jitter rendah, dan packet loss minimal pada skenario trafik intensif, menunjukkan overhead enkapsulasi yang terkendali. Analisis MITM mengonfirmasi ketahanan autentikasi PSK terhadap inspeksi payload dan modifikasi paket, meskipun rentan jika pengelolaan kunci longgar. Pengujian DoS mengungkap penurunan throughput hingga 1.8 Mbps dengan latency 79 ms dan packet loss 14% akibat SYN/ICMP flood, tanpa kolaps kanal VPN. Grafik korelasi menampilkan fluktuasi intensitas serangan paralel degradasi performa. L2TP/IPsec direkomendasikan untuk layanan real-time dengan penguatan manajemen PSK, rate limiting, dan IDS/IPS. Penelitian lanjutan disarankan membandingkan dengan WireGuard dan IKEv2 pada topologi multipoint.

Kata Kunci*: L2TP/IPsec, serangan MITM, DoS, QoS, throughput TCP, autentikasi PSK*

Abstract

This study assesses the performance and security resilience of L2TP/IPsec protocol against Man-in-the-Middle (MITM) and Denial of Service (DoS) attacks in PT. XYZ's network environment. QoS evaluations recorded throughput in tens of Mbps, low jitter, and minimal packet loss under intensive traffic scenarios, indicating controlled encapsulation overhead. MITM analysis confirmed PSK authentication resilience against payload inspection and packet modification, albeit vulnerable to lax key management. DoS tests revealed throughput degradation to 1.8 Mbps, with 79 ms latency and 14% packet loss from SYN/ICMP floods, without VPN tunnel collapse. Correlation graphs depicted attack intensity fluctuations paralleling performance degradation. L2TP/IPsec is recommended for real-time services, augmented by stringent PSK management, rate limiting, and IDS/IPS. Further research suggests comparisons with WireGuard and IKEv2 in multipoint topologies..

Keywords*: L2TP/IPsec, MITM attack, DoS, QoS, TCP throughput, PSK authentication.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi membuat organisasi semakin bergantung pada jaringan publik untuk mendukung kolaborasi dan pertukaran data antar lokasi. Dalam konteks tersebut, penggunaan internet sebagai media utama komunikasi menghadirkan risiko serius terhadap kerahasiaan, integritas, dan ketersediaan data, terutama akibat serangan seperti sniffing, man-in-the-middle (MITM), dan eksploitasi celah keamanan yang dapat memicu kebocoran informasi strategis [1], [2], [3]. VPN kemudian menjadi mekanisme kunci untuk mengamankan komunikasi melalui teknik tunneling dan enkripsi, sehingga lalu lintas data yang melewati jaringan publik terlindungi dari intersepsi langsung [4].

Berbagai studi menunjukkan bahwa penerapan VPN mampu meningkatkan keamanan jaringan secara signifikan, namun konsekuensinya adalah penurunan performa yang tidak dapat diabaikan. [5] melaporkan bahwa VPN dapat meningkatkan keamanan akses hingga sekitar 65%, disertai penurunan performa sekitar 22%, bergantung pada protokol dan kondisi jaringan yang digunakan. Temuan ini sejalan dengan kajian lain yang menegaskan adanya trade-off antara keamanan dan kualitas layanan, sehingga dibutuhkan evaluasi kuantitatif terhadap stabilitas dan QoS sebelum VPN dioperasikan pada lingkungan produksi.

Literatur keamanan jaringan juga menekankan bahwa ancaman tidak hanya berasal dari luar, tetapi sangat dipengaruhi oleh kelemahan desain dan konfigurasi internal [1], [6]. Dalam ranah ini, kombinasi L2TP dengan IPSec (L2TP/IPSec) menjadi salah satu solusi VPN yang banyak diadopsi karena kompatibilitas luas, dukungan enkripsi serta autentikasi yang kuat, dan performa yang relatif stabil pada parameter QoS seperti throughput, delay, jitter, dan packet loss [7], [8].Namun, overhead enkripsi dan pengaturan kunci yang kompleks membuat konfigurasi yang tidak tepat berpotensi menimbulkan kerentanan baru, termasuk terhadap serangan MITM dan Denial of Service (DoS) [7], [9].

Berangkat dari konteks tersebut, analisis terarah terhadap dampak serangan MITM dan DoS pada protokol L2TP/IPSec menjadi sangat relevan, khususnya ketika organisasi seperti PT. XYZ mengandalkan VPN sebagai tulang punggung komunikasi data yang aman dan berkelanjutan. Penelitian ini berfokus mengevaluasi bagaimana kedua jenis serangan tersebut memengaruhi parameter QoS koneksi L2TP/IPSec, sekaligus menilai sejauh mana mekanisme enkripsi, autentikasi, dan manajemen trafik pada protokol ini mampu menjaga kualitas layanan di tengah kondisi jaringan yang terpapar ancaman [10].

2. METODE PENELITIAN

Tahap penelitian ini dirancang untuk menghasilkan evaluasi yang sistematis terhadap dampak serangan Man-in-the-Middle (MITM) dan Denial of Service (DoS) pada protokol L2TP/IPSec dengan meninjau aspek Quality of Service (QoS). Langkah awal adalah identifikasi masalah, di mana peneliti memetakan kebutuhan PT. XYZ akan koneksi VPN yang aman sekaligus stabil untuk komunikasi data antar-cabang. Pada tahap ini juga diidentifikasi kebutuhan mitigasi teknis sebelum layanan VPN diimplementasikan penuh pada jaringan operasional perusahaan, sehingga risiko gangguan layanan dan kompromi keamanan dapat diminimalkan.

Tahap berikutnya adalah pengumpulan data awal melalui studi literatur dan dokumentasi teknis terkait VPN, protokol L2TP/IPSec, perangkat Mikrotik, modem Bivocom/Raisecom, perangkat analisis jaringan (Wireshark, iPerf3), serta parameter QoS dan konsep keamanan jaringan. Kajian literatur ini dilengkapi dengan dokumen konfigurasi VPN yang digunakan PT. XYZ dan panduan resmi dari vendor perangkat, sehingga rancangan eksperimen merefleksikan kondisi nyata di lapangan dan bukan sekadar simulasi generik.

Setelah itu, dilakukan perancangan topologi jaringan berbasis testbed. Mikrotik Router dikonfigurasikan sebagai server VPN utama yang melayani koneksi L2TP/IPSec. Jaringan publik dimodelkan sebagai cloud/internet, sementara Bivocom dan Raisecom berperan sebagai klien VPN yang merepresentasikan akses dari jaringan seluler atau media publik lainnya. Beberapa PC disusun dengan peran berbeda: PC-1 sebagai jaringan lokal perusahaan, PC-2 sebagai endpoint pengguna, PC-3 sebagai mesin uji performa dan keamanan di sisi klien, dan PC-4 sebagai mesin monitoring di sisi server. Desain ini memungkinkan pengamatan menyeluruh terhadap jalur komunikasi mulai dari LAN internal hingga akses publik.

Tahap konfigurasi dan simulasi berfokus pada penerapan L2TP/IPSec di Mikrotik menggunakan antarmuka manajemen (Winbox/CLI). Konfigurasi meliputi pengaturan IP addressing, pembuatan tunnel L2TP dengan proteksi IPSec, manajemen sertifikat atau kredensial autentikasi, penentuan IP-Pool untuk klien, serta penyesuaian aturan firewall dan NAT agar trafik terenkripsi dapat dilewatkan dan dimonitor. Setelah koneksi VPN stabil, dilakukan skenario uji performa menggunakan iPerf3 dan Wireshark untuk memotret throughput, latency, jitter, dan packet loss, baik pada trafik rendah, sedang, maupun pada trafik yang dimaksimalkan sesuai kapasitas link.

Untuk menguji ketahanan keamanan, dirancang skenario serangan terkontrol. Pengujian sniffing dilakukan dengan Wireshark untuk melihat visibilitas payload pada jalur tanpa VPN dan pada tunnel L2TP/IPSec. Serangan MITM disimulasikan menggunakan tools seperti Ettercap untuk melakukan ARP spoofing dan penyisipan trafik, sehingga dapat dievaluasi apakah integritas dan kerahasiaan data tetap terjaga. Serangan DoS dilancarkan dengan generator trafik (misalnya hping3) untuk membanjiri server VPN selama interval tertentu, sementara parameter QoS diukur secara paralel untuk melihat degradasi throughput dan peningkatan delay/jitter. Jika diperlukan, dilakukan pula uji replay untuk menilai apakah server menerima atau menolak paket duplikat yang dikirim ulang.

Data penelitian yang diperoleh dibagi menjadi data primer dan sekunder. Data primer berupa hasil pengukuran numerik QoS (throughput, latency, jitter, packet loss) dan indikator keamanan (log autentikasi, status sesi VPN, hasil serangan sniffing, MITM, DoS) yang dihasilkan langsung dari eksperimen testbed. Data sekunder berasal dari publikasi ilmiah dan dokumentasi terdahulu yang membahas performa dan keamanan protokol VPN, yang digunakan sebagai rujukan pembanding dan dasar teori.

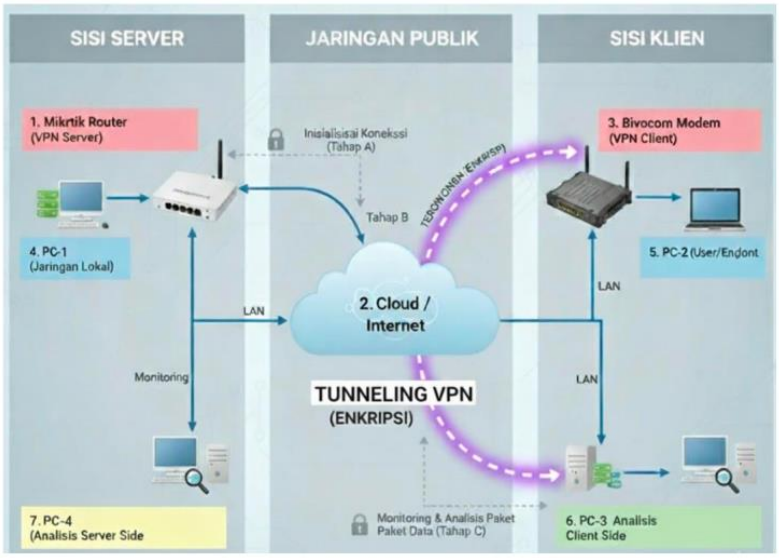
Teknik pengumpulan data lapangan meliputi wawancara dengan tim teknis PT. XYZ, observasi pola trafik dan kondisi jaringan, serta pengumpulan dokumen konfigurasi dan prosedur operasional standar yang terkait penggunaan VPN. Wawancara digunakan untuk menegaskan kebutuhan bisnis dan kendala yang sering terjadi (misalnya fluktuasi stabilitas, batasan bandwidth, dan kebijakan keamanan), sehingga skenario uji selaras dengan kebutuhan nyata organisasi.

Metode yang digunakan bersifat eksperimental kuantitatif dan komparatif. Peneliti membangun lingkungan uji terkontrol, menjalankan rangkaian eksperimen dengan variasi skenario trafik dan serangan, lalu mengumpulkan data numerik yang dianalisis secara

statistik dan dibandingkan dengan standar QoS (misalnya TIPHON/ITU-T) serta temuan literatur. Analisis akhir dilakukan dengan memetakan pengaruh serangan MITM dan DoS terhadap kinerja L2TP/IPSec dari sisi QoS dan keamanan. Hasilnya kemudian digunakan untuk menyusun rekomendasi teknis bagi PT. XYZ mengenai kelayakan penggunaan L2TP/IPSec, batasan performa yang realistis, dan mekanisme mitigasi yang perlu diterapkan agar koneksi VPN tetap aman dan stabil di lingkungan jaringan produksi.

3. HASIL DAN PEMBAHASAN

Alur koneksi mengalir dari Sisi Server melalui tunnel enkripsi di Jaringan Publik menuju Sisi Klien, dengan panah biru tebal menandakan enkripsi tunneling dan panah lainnya menunjukkan akses modem serta monitoring. Komponen monitoring terletak di kedua sisi (server dan client), dengan PC1, PC2, PC3, serta router/modem sebagai node utama; tidak ada label numerik kuantitatif seperti satuan waktu atau throughput pada diagram. Sebagaimana ditunjukkan pada Gambar 1, posisi "Monitoring & Analisis Paket" di sisi server dan client mendukung pengamatan lalu lintas paket melalui tunnel enkripsi, sementara label "Mikrotik Router (VPN Server)" dan "PC Client" mengilustrasikan distribusi node LAN di zona terpisah oleh jaringan publik.



Gambar 1. Konfigurasi eksperimen penelitian

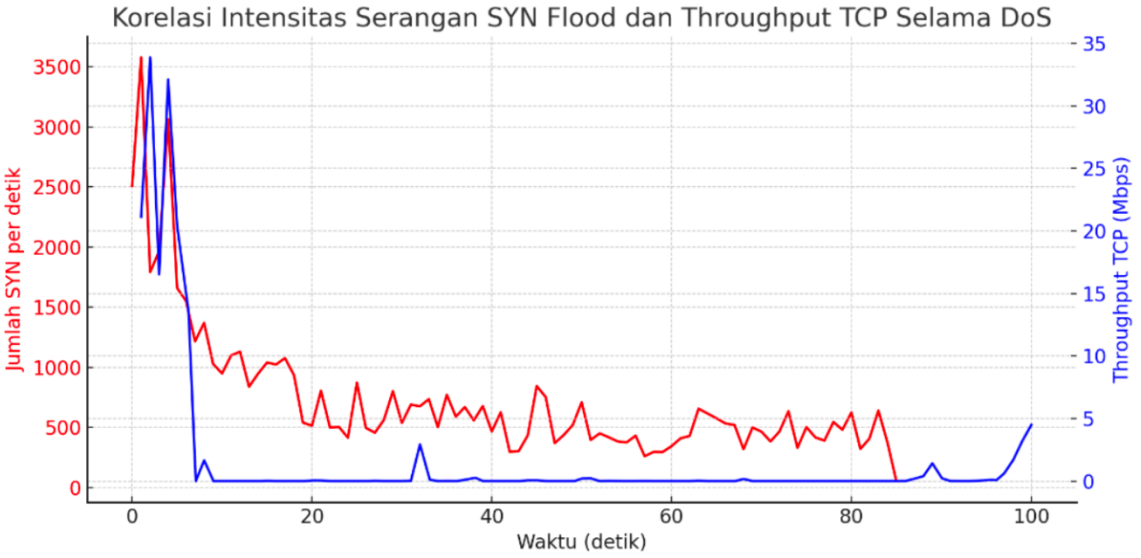
3.3. Analisa QoS saat terjadi Serangan DoS pada L2TP/IPSEC

Data menunjukkan durasi serangan mencapai 86 detik dengan total paket SYN sebanyak 62.603, di mana puncak SYNs mencapai 3.577 dan rata-rata SYNs sebesar 727.94. Throughput TCP rata-rata turun menjadi 1.59 Mbps, disertai overhead 89.68, yang mengindikasikan beban tinggi pada protokol selama serangan. Rentang throughput TCP rata-rata 1.59 Mbps dengan overhead 89.68 mencerminkan penurunan performa jaringan akibat volume SYN yang tinggi (rata-rata 727.94 per satuan waktu), sebagaimana ditunjukkan pada Tabel 1.

TABEL 1. Serangan DoS pada L2TP/IPSEC

Parameter	Nilai
Total Paket SYN	62.603
Durasi (detik)	86
Puncak SYN/s	3.577
Rata-rata SYN/s	727.94
Rata-rata throughput TCP (Mbps)	1.59
Overhead	89.68%

Garis merah (SYN) memulai pada ~0, melonjak tajam ke puncak ~3500 pada awal, kemudian turun fluktuatif hingga mendekati 0 pada 100 detik. Garis biru mulai 30-35 Mbps, mengalami penurunan tajam ke 0 bersamaan dengan lonjakan SYN, dan tetap rendah fluktuatif selama periode tersebut; pola menunjukkan penurunan throughput simultan karena fungsi throughput yang tinggi. Gambar 2 menunjukkan lonjakan SYN hingga 3500 per detik yang bertepatan dengan penurunan TCP throughput menjadi 35 Mbps ke 0 Mbps dalam 0-20 detik, diikuti oleh fluktuasi rendah selama 100 detik untuk keduanya..



Gambar 2. DoS pada SYN di L2TP/IPSEC

3.4. Analisa Serangan MITM pada L2TP/IPSEC

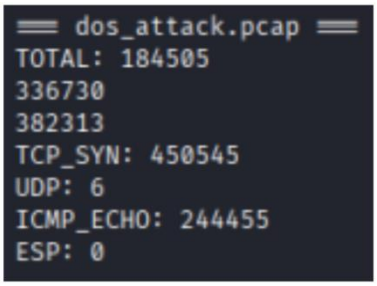
Semua aspek menunjukkan ketahanan protokol, di mana payload aplikasi tidak terlihat, data sensitif tidak muncul, inspeksi MITM tidak mungkin, modifikasi paket tidak mungkin, dan deteksi replay didukung Anti-Replay IPsec. Tidak ada anomali yang menunjukkan kebocoran data. Tabel 2 memperlihatkan nol keberhasilan pada kelima aspek MITM, menegaskan integritas paket terjaga tanpa modifikasi atau inspeksi yang berhasil.

TABEL 2. Serangan MITM pada L2TP/IPSEC

Aspek	L2TP/IPSEC
Payload Aplikasi(HTTP/HTTPS/Winbox)	Tidak terlihat
Data Sensitif (Username/Password)	Tidak muncul
Inspection via MITM	Tidak bisa
Integrity/Modifikasi Paket	Tidak mungkin
Replay detection	Anti-Replay IPsec

3.5. Analisa Serangan DoS pada L2TP/IPSEC

Hasil Analisis pengujian terhadap DOS dengan semua jenis pengujian DOS berupa SYN Flood, ICMP Flood, UDP Flood, serta timeout. Hasil uji ping klien ke Server L2TP/IPSec mencatat rata-rata latensi 79 ms dengan Packet Loss sebesar 14%, yang menandakan gangguan serius pada kemampuan router dalam memproses paket.



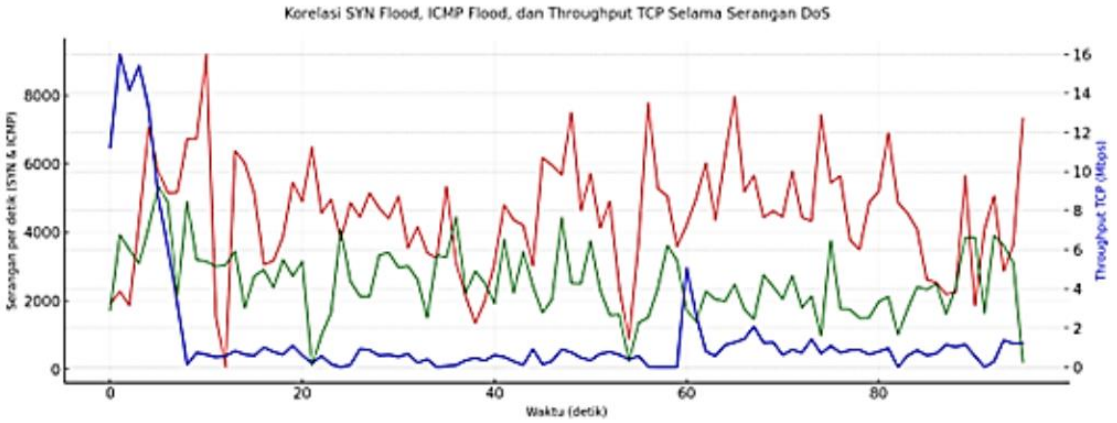
Gambar 3. Ringkasan analisa serangan DoS pada file PCAP

SYNs menunjukkan variasi dari minimum 64 hingga maksimum 9.194 dengan rata-rata 4.475, sementara ICMPs berkisar 110 hingga 5.346 (rata-rata 2.760). Throughput TCP bervariasi luas dari 0.0 Mbps hingga 15.5 Mbps, dengan rata-rata 1.8 Mbps. Selisih throughput TCP dari 0.0 Mbps (minimum) hingga 15.5 Mbps (maksimum) dengan rata-rata 1.8 Mbps pada Tabel 3 menggambarkan fluktuasi performa ekstrem selama serangan DoS.

TABEL 3. Hasil temuan pengujian serangan DoS

Parameter	Nilai Minimum	Nilai Maksimum	Rata-rata
SYN/s	64	9.194	4.475
ICMP/s	110	5.346	2.760
Throughput TCP (Mbps)	0.0	15.5	1.8

Pada gambar 4, Garis biru (SYN) dan merah (ICMP) menunjukkan fluktuasi tinggi dengan puncak SYN ~8000 dan ICMP ~6000-7000 per detik di awal, kemudian osilasi tajam hingga akhir periode. Garis hijau (throughput) fluktuatif antara positif rendah (~2-10 Mbps) dan negatif (~-2 hingga -14 Mbps), dengan pola osilasi paralel lonjakan flood; tidak ada tren monoton keseluruhan.



Gambar 4. Performa serangan DoS di L2TP/IPSEC

Untuk MITM, justifikasi menegaskan aman secara aktif dan pasif tanpa payload terbaca atau modifikasi. Untuk DoS, latency rata-rata 79 ms dan packet loss 14% disertai throughput 1.8 Mbps (penurunan 90%) menunjukkan penurunan availability meskipun data tidak bocor. Penurunan throughput TCP hingga 1.8 Mbps dengan packet loss 14 pada aspek DoS di Tabel 4 mendukung kerentanan availability, kontras dengan ketahanan MITM di mana integritas paket terjaga sepenuhnya.

TABEL 4. Hasil temuan pengujian serangan MITM dan DoS

Aspek Pengujian	L2TP/IPSEC	Justifikasi
MITM	Tidak ada payload terbaca, data sensitif tidak muncul, packet integrity terjaga, anti-replay aktif	Aman dari MITM secara aktif (modifikasi paket) maupun pasif
DoS	Rata-rata latency 79 ms, Packet Loss 14%, TCP throughput turun menjadi 1.8 Mbps (penurunan>90%), rentan terhadap SYN/ICMP Flood	Data tidak bocor ketika serangan terjadi, namun availability menurun signifikan

4. KESIMPULAN

Hasil rangkaian pengujian menunjukkan bahwa karakteristik kinerja dan ketahanan keamanan protokol L2TP/IPSec pada lingkungan jaringan PT. XYZ sangat dipengaruhi oleh kondisi trafik serta jenis serangan yang disimulasikan. Dari perspektif kualitas layanan (Quality of Service), L2TP/IPSec secara konsisten mampu mempertahankan nilai throughput yang tinggi, jitter rendah, dan packet loss yang minimal pada berbagai skenario beban, mulai dari trafik rendah hingga mendekati kapasitas maksimum tautan. Stabilitas ini menunjukkan bahwa mekanisme enkapsulasi dan enkripsi pada L2TP/IPSec menghasilkan overhead yang masih terkendali, sehingga kanal VPN tetap andal untuk layanan yang sensitif terhadap waktu, seperti monitoring real-time dan pertukaran data operasional antarsitus.

Pada skenario trafik intensif, ketika jaringan berada dalam kondisi mendekati saturasi, L2TP/IPSec tetap menunjukkan kemampuan transmisi yang relatif stabil. Throughput yang dicapai berada pada kisaran puluhan megabit per detik dan degradasi performa yang

muncul masih berada dalam batas yang dapat ditoleransi untuk operasi bisnis kritis. Jitter dan packet loss pada umumnya tetap rendah, sehingga pola distribusi paket tidak mengalami fluktuasi ekstrem meskipun terjadi lonjakan beban dan injeksi serangan. Kondisi ini mengindikasikan bahwa pipeline pemrosesan paket pada sisi server dan klien L2TP/IPSec cukup efisien, sehingga tidak mudah mengalami bottleneck saat dihadapkan pada skenario beban puncak.

Dari sisi keamanan, pengujian serangan Man-in-the-Middle (MITM) memperlihatkan bahwa ketahanan L2TP/IPSec sangat bergantung pada kekuatan skema autentikasi yang digunakan, khususnya dalam pengelolaan Pre-Shared Key (PSK). Apabila PSK tidak dikelola secara ketat, misalnya dibagikan ke banyak pihak atau tidak diganti secara berkala, risiko kompromi kredensial meningkat dan membuka peluang bagi penyerang untuk melakukan penyusupan atau rekonstruksi sesi tunnel. Temuan ini menegaskan bahwa konfigurasi dan tata kelola kunci menjadi komponen krusial dalam mempertahankan integritas koneksi L2TP/IPSec.

Pengujian Denial of Service (DoS) menunjukkan pola yang berbeda. Ketika server L2TP/IPSec dibanjiri trafik berlebih melalui flood paket, performa memang mengalami penurunan, namun kanal VPN tidak langsung kolaps. Throughput masih dapat dipertahankan pada level tertentu dan server tetap mampu memproses sebagian koneksi sah, meskipun terjadi peningkatan delay dan jitter. Hal ini mengindikasikan bahwa stack L2TP/IPSec relatif lebih tangguh terhadap serangan saturasi dibandingkan skenario yang umumnya terlihat pada protokol tunneling lain yang lebih berat dari sisi komputasi. Namun, jika intensitas serangan terus ditingkatkan atau tidak diimbangi mekanisme proteksi tambahan, layanan tetap berpotensi mengalami degradasi signifikan.

Secara keseluruhan, hasil pengukuran throughput, jitter, dan packet loss selama serangan MITM maupun DoS memperlihatkan bahwa L2TP/IPSec menawarkan profil performa yang seimbang antara kualitas transmisi dan ketahanan layanan. Protokol ini lebih sesuai untuk skenario operasional di PT. XYZ yang menuntut kestabilan koneksi dan kapasitas transfer data tinggi, khususnya pada trafik antar-cabang dan layanan pemantauan yang berjalan terus-menerus. Namun, dari sisi keamanan tingkat lanjut, terutama terkait perlindungan terhadap MITM yang memanfaatkan kelemahan autentikasi, L2TP/IPSec memerlukan penguatan melalui praktik manajemen kunci yang baik, pemanfaatan sertifikat digital, serta integrasi dengan mekanisme deteksi intrusi.

Berdasarkan temuan tersebut, rekomendasi teknis untuk PT. XYZ adalah menempatkan L2TP/IPSec sebagai protokol utama pada layanan yang berorientasi performa dan kestabilan QoS, misalnya komunikasi antar-site, replikasi data, dan sistem pemantauan real-time. Implementasi perlu disertai kebijakan pengelolaan Pre-Shared Key yang ketat, rotasi berkala kredensial, serta segmentasi akses bagi setiap kelompok pengguna. Selain itu, penerapan aturan firewall yang lebih granular, penggunaan teknik rate limiting pada trafik yang mencurigakan, dan integrasi dengan sistem IDS/IPS akan memperkuat ketahanan terhadap serangan DoS yang berpotensi menguras sumber daya server VPN.

Untuk pengembangan penelitian, disarankan pengujian lanjutan yang membandingkan L2TP/IPSec dengan protokol lain seperti WireGuard atau IKEv2/IPSec dalam skenario serangan MITM dan DoS yang lebih beragam. Pengujian pada topologi multipoint atau multi-site, serta pada berbagai kelas media transmisi (fiber, seluler, dan satelit), juga akan memberikan gambaran yang lebih komprehensif mengenai perilaku QoS dan keamanan VPN di lingkungan produksi yang kompleks. Dengan pendekatan tersebut, hasil penelitian dapat memberikan kontribusi yang lebih luas terhadap pemetaan trade-off antara keamanan, performa, dan skalabilitas pada implementasi VPN korporat modern.

DAFTAR PUSTAKA

[1] A. Bustami and S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review," *UNISTEK*, vol. 7, no. 2, pp. 59–70, Aug. 2020, doi: 10.33592/unistek.v7i2.645.

[2] R. Rahman and A. Y. N. Leksona, "Serangan Man-In-The-Middle (MITM) di Jaringan Publik: Studi dan Solusi Simulasi Serangan Password Cracking Menggunakan Hydra," *Jurnal Ilmiah Multidisiplin*, vol. 1, no. 4b, 2025.

[3] R. Setiawan, R. Sufri, and R. Hermanto, "Analisis Keamanan Jaringan Terhadap Serangan Packet Sniffing Menggunakan Wireshark, Ettercap dan PCAP-Droid," *Jurnal Ristech (Jurnal Riset, Sains dan Teknologi)*, vol. 6, no. 2, 2025.

[4] H. Pribadi Fitrian, N. Alia Destiara, N. Elsa Destianti, and G. Maddanil Khowat, "ANALISIS PENERAPAN TEKNOLOGI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI KEAMANAN DATA DI JARINGAN PUBLIK," *jati*, vol. 9, no. 1, pp. 1559–1563, Jan. 2025, doi: 10.36040/jati.v9i1.12712.

[5] T. S. Ali, I. Santoso, and A. S. Quiko, "PENGARUH VIRTUAL PRIVATE NETWORK (VPN) TERHADAP KEAMANAN DAN PERFORMA AKSES JARINGAN," *JAREKOM: Jurnal Rekayasa Komputer*, vol. 01, no. 01, 2025.

[6] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *AITI*, vol. 17, no. 2, pp. 143–158, Feb. 2021, doi: 10.24246/aiti.v17i2.143-158.

[7] S. Ilmare, "Analisis Quality of Service Protokol VPN Berbasis Mikrotik RouterOS pada Lingkungan GNS3 dengan Standar TIPHON dan Model ITU-T G-107 pada IPv6 Menggunakan Tunneling 6to4," *IK*, vol. 18, no. 3, pp. 83–92, Dec. 2024, doi: 10.56706/ik.v18i3.111.

[8] M. Khofikur R.A, F. P. Eka Putra, Moh. W. Ridho G, and V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," *INFOTEK*, vol. 8, no. 2, pp. 334–344, Jul. 2025, doi: 10.29408/jit.v8i2.30230.

[9] Y. W, Yuliadi, F. Hamdani, Y. Bella Fitriana, and N. Oper, "Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 3, no. 6, 2023.

[10] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, "Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi," *jipi. jurnal. ilmiah. penelitian. dan. pembelajaran. informatika.*, vol. 9, no. 4, pp. 2357–2364, Nov. 2024, doi: 10.29100/jipi.v9i4.6943.