Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

ANALISIS DAN IMPLEMENTASI INTERKONEKSI JARINGAN KOMPUTER BERBASIS VPNL2TP IPSEC PADA SMK TKJ DI DEPOK

Ali Imran[1] , April Rustianto[2]

[1, 2]Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri
Jakarta Selatan, DKI Jakarta, Indonesia 12640
aliimran@student.nurulfikri.ac.id , april.rustianto@nurulfikri.ac.id

Abstract

The world of education, especially in Vocational School Computer and Network Engineering (TKJ) schools at Depok, requires technology to support learning and teaching activities digitally or online. Currently, schools are connected via an internet connection, but there are problems related to data security when exchanging data between schools. In this research, IT infrastructure was built relating to the interconnection of computer networks in TKJ schools at Depok to connect schools with multilevel security. The method used observation, interviews, and literature to analyze the network needed and make a design to be implemented and tested from the results of the implemented design. The results of this study were successful in connecting SMK TKJ schools at Depok with Virtual Private Network (VPN) technology based on Layer 2 Tunneling Protocol (L2TP) and IP Security optimally, which has been tested. So, I concluded that the design and implementation of L2TP and IPSec VPNs could be worked well to connect between SMK TKJ at Depok.

Keywords: *VPN, L2TP, IPSec, Network Interconnection*

Abstrak

Dunia pendidikan terkhusus di sekolah-sekolah SMK Teknik Komputer dan Jaringan (TKJ) Se-Depok memerlukan teknologi untuk menunjang sarana kegiatan belajar dan mengajar secara digital atau daring. Saat ini sekolah-sekolah terhubung melalui koneksi internet, namun terdapat masalah terkait keamanan data ketika melakukan pertukaran data antar sekolah. Pada penelitian ini dibangun infrastruktur IT terkait interkoneksi jaringan komputer di sekolah TKJ Se-Depok agar dapat terhubung antar sekolah dengan keamanan yang bertingkat. Metode yang digunakan adalah metode observasi, wawancara, dan literatur untuk menganalisa jaringan yang dibutuhkan serta membuat rancangan untuk diimplementasikan dan akan dilakukan pengujian dari hasil rancangan yang diimplementasikan. Hasil penelitian ini adalah berhasil menghubungkan sekolah SMK TKJ Se-Depok dengan teknologi *Virtual Private Network* (VPN) berbasis *Layer 2 Tunneling Protokol* (L2TP) dan IP *Security* secara optimal yang telah diujikan, sehingga saya simpulkan bahwa rancangan dan implementasi VPN L2TP dan IPSec dapat berjalan dengan baik untuk menghubungkan antar SMK TKJ Se-Depok.

Kata kunci: VPN, L2TP, IPSec, Interkoneksi Jaringan

1. PENDAHULUAN

Perkembangan teknologi dan jaringan komputer saat ini telah memberikan dampak yang signifikan bagi efisiensi pekerjaan manusia. Dalam dunia pendidikan, teknologi juga sangat diperlukan terkhusus di sekolah SMK jurusan Teknik Komputer dan Jaringan (TKJ) Se-Depok yang digunakan untuk menunjang sarana kegiatan belajar dan mengajar secara digital atau secara daring. Kondisi saat ini sekolah-sekolah sudah terkoneksi antar sekolah menggunakan internet, namun menimbulkan masalah baru terkait tingkat keamanan yang kurang baik terhadap pertukaran data yang dilakukan oleh antar sekolah SMK TKJ Se-Depok. Sebagaimana cita-cita dari para guru SMK TKJ Se-Depok yang tergabung dalam satu organisasi yang bernama MGMP TKJ Depok yang menginginkan setiap sekolah dapat terhubung secara lokal dan memiliki tingkat keamanan yang baik, maka penelitian ini berfokus untuk melakukan penghubungan jaringan atau dalam kata lain disebut juga interkoneksi jaringan yang mana peneliti memilih *Virtual Private Network* (VPN) sebagai inti teknologi yang digunakan untuk menghubungkan antar sekolah SMK TKJ Se-Depok dan ditambah dengan teknik *routing* untuk pengenalan jaringan disetiap sekolah. Berdasarkan uraian latar belakang yang sudah disebutkan, maka hal-hal yang diperlukan mengenai interkoneksi jaringan antar sekolah menggunakan VPN didapatkan rumusan masalah utama

Diterima 20 Januari 2021, Direvisi 26 Februari 2021, Diterima untuk publikasi 19 Maret 2021

yaitu: Bagaimana merancang dan mengimplementasikan teknologi VPN menggunakan L2TP dan IPSec dengan *routing* OSPF yang terkoneksi dengan internet dan bagaimana kemampuan jaringan VPN ini untuk digunakan sebagai alat penghubung antar sekolah TKJ Se-Depok. Dengan begitu tujuan dari penelitian ini adalah menyelesaikan masalah utama setiap sekolah yang ingin terkoneksi satu sama lain dengan aman. Penelitian ini memeliki batasan-batasan masalah yang bertujuan untuk lebih terarah dan fokus dalam menyelesaikan permasalahan yang ada, ialah: Penelitian ini tidak menjelaskan bagaimana teknik enkripsi dan tidak membahas keseluruhan terkait kemampuan jaringan VPN yang dibangun.

Virtual Private Network (VPN) itu sendiri adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal [1]. Dalam pengertian lain VPN juga berarti teknik pengamanan jaringan yang berkerja dengan cara membuat suatu *tunnel* sehingga jaringan yang dipercaya dapat menghubungkan jaringan yang ada diluar melalui internet [2]. Ada berbagai macam protokol pada VPN yang bisa diterapkan salah satunya adalah protokol *Layer 2 Tunneling Protocol* (L2TP).

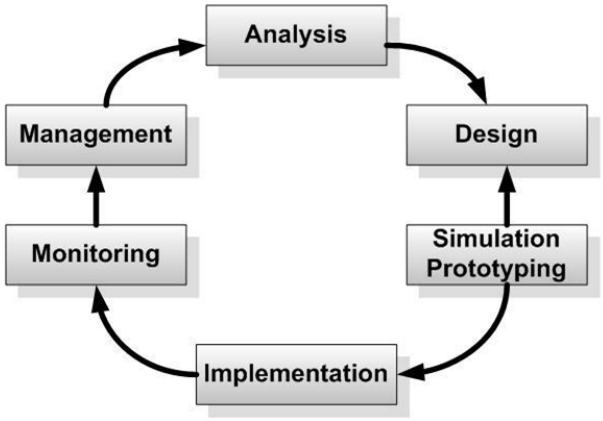
L2TP merupakan *tunneling protocol* yang memadukan dua buah *tunneling* milik Cisco dan PPTP yang dimiliki Microsoft [3]. Dalam teori lain L2TP adalah *tunneling* yang berkerja pada *layer 2*, tetapi tidak memiliki pengamanan khusus sehingga biasanya ditambahkan sistem kemanan yang lebih baik, yaitu menggunakan IPSec [4]. Sedangkan *tunneling* itu sendiri adalah teknologi terowongan dalam jaringan yang berfungsi menhubungkan dengan jaminan keamanan yang baik menggunakan enkripsi.

IPSec adalah satu kerangka kerja dari satu set protokol-protokol untuk keamanan pada jaringan atau paket yang diproses pada lapisan dari jaringan komunikasi [5]. IPSec ini berguna untuk meningkatkan keamanan berlapis untuk jaringan *Virtual Private Network* (VPN) L2TP yang diimplementasikan. IPSec memberikan perlindungan ganda melalui otentikasi [6], dengan teknik otentikasi dan enkripsi pada setiap kali mengirimkan data antar jaringan IPSec akan memberikan keamanan yang baik agar terhindar dari hal-hal kejahatan dalam jaringan seperti penyadapan data atau dikenal dengan istilah *sniffing packet*.

Routing merupakan proses untuk meneruskan paket yang dikirim dan digunakan untuk memilih jalur dari sebuah jaringan. Jenis dari *routing* ada beragam, ada yang statis dan dinamis. Sedangkan *routing* OSPF itu sendiri merupakan salah satu dari jenis *routing* yang tersedia, masuk dalam kategori *routing* dinamis. *Open Shortest Path First* (OSPF) adalah sebuah *routing protocol* yang dipergunakan untuk merutekan paket data yang akan dikirimkan dari sebuah komputer ke komputer lain dalam jaringan komputer [7].

2. METODE PENELITIAN

Metode yang digunakan pada penelitian ini adalah menggunakan *Network Development Life Cycle* (NDLC), merupakan metode yang digunakan untuk pembangunan atau pengembangan yang dilakukan dengan berbagai proses seperti melalukan *analysis, design, simulation prototyping, implementation, monitoring,* dan *management.* Gambar 1 menunjukan proses dari metode NDLC.



Gambar 1. Proses NDLC

2.1 Metode Pengumpulan Data

Dalam melakukan pengumpulan data, peneliti melakukan analisis sesuai kebutuhan penelitian dan sesuai dari tahapan NDLC ialah sebagai berikut:

1. Observasi
   Tahap ini peneliti melakukan pengamatan langsung terhadap kondisi jaringan yang sudah berjalan sebelumnya dan melalukan analisa rancangan topologi yang akan diimplementasikan.
2. Studi Pustaka
   Pada tahap ini peneliti mengumpulkan data-data pendukung dan mengkaji literatur beserta laporan yang berkaitan dengan penelitian yang sedang dikerjakan.
3. Wawasan dan Diskusi
   Pada tahap ini peneliti melakukan wawancara dan diskusi langsung terhadap para guru TKJ Se-Depok yang tergabung dalam organisasi MGMP untuk meminta masukan dalam perancangan dan pembangunan jaringan interkoneksi VPN ini.

Dalam melakukan pengujian pada penelitian ini ada beberapa *point* yang difokuskan dan dibahas, antara lain sebagai berikut:

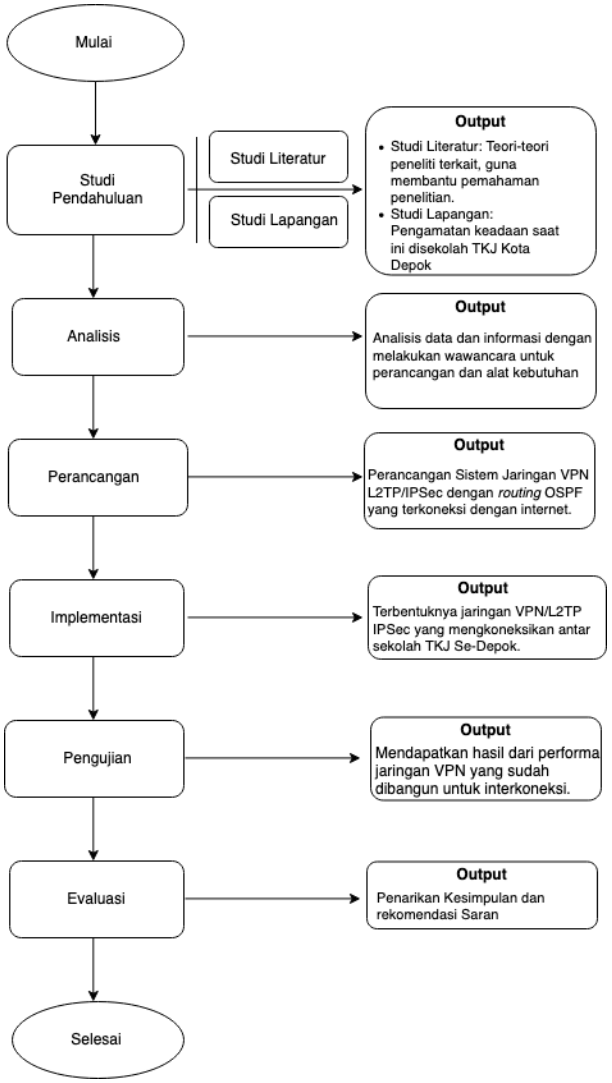
a. *Delay*
   Untuk melihat performa dari jaringan VPN yang dibangun pada penelitian ini, peneliti mengukur nilai dari *delay* didalam jaringan tersebut. *Delay* adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan [3].

b. *Jitter*
Selain *delay* yang diuji untuk melihat performa dari jaringan VPN L2TP dan IPSec ini juga diukur nilai *jitter* yang merupakan kumpulan dari semua *delay* yang terjadi selama proses pengiriman data sampai dengan penerimaan data [8]

c. *Packet Loss*
Dan *point* berikutnya yang diujikan pada penelitian adalah melihat nilai dari *packet loss* untuk mengukur seberapa baik paket yang dilewati dalam jaringan VPN tersebut. Sedangkan *packet loss* sendiri merupakan parameter yang menggambarkan suatu kondisi yang menunjukan jumlah total paket yang hilang [8].

d. *Sniffing*
Dan *point* terakhir yang diujikan dari sisi keamanan adalah dengan teknik *sniffing* paket data yang melewati jaringan VPN. *Sniffing* itu sendiri merupakan teknik dalam keamanan jaringan untuk menangkap lalu lintas data yang aktif pada jaringan untuk dilakukan penyadapan

2.2 Tahapan Penelitian



Gambar 2. Tahapan Penelitian

Berikut adalah penjelasan dari tahapan penelitian yang dilakukan:

a. Studi Pendahuluan
Tahapan ini peneliti mencari bahan literatur berupa teori-teori terkait penelitian yang sedang dibangun dan juga melalukan studi lapangan setelah mencari pemahaman teori dari literatur yang dikumpulkan untuk melihat kondisi sekolah TKJ Se-Depok.

b. Analisis
Tahapan ini peneliti mencari informasi lebih *detail* kepada para guru TKJ Se-Depok dengan cara wawancara terkait penelitian yang sedang dibangun.

c. Perancangan
Tahapan ini peneliti sudah mendapatkan berbagai informasi yang selanjutnya dibuat rancangan-rancangan untuk membangun jaringan VPN L2TP/IPSec.

d. Implementasi
Tahapan implementasi merupakan langkah untuk mengerjakan semua rancangan yang sudah dibuat agar interkoneksi jaringan antar sekolah dapat terealisasikan.

e. Pengujian
Tahap ini peneliti melakukan pengujian dari beberapa *point* yang sudah disebutkan sebelumnya, yaitu: *Delay, Jitter, Packet Loss.*

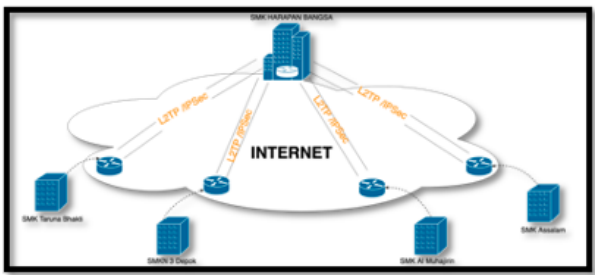
f. Evaluasi
Tahap terakhir dari penelitian ini adalah penarikan kesimpulan dan saran untuk penelitian berikutnya yang ingin membangun teknologi yang serupa.

3. HASIL DAN PEMBAHASAN

Berdasarkan tahapan-tahapan yang sudah dijelaskan sebelumnya, peneliti paparkan pembahasan dan hasilnya sebagai berikut:

3.1 Pembahasan Penelitan

a. Rancangan Topologi
Dari pengumpulan data yang dilakukan oleh peneliti untuk membangun jaringan VPN ini, dibuatlah rancangan topologi jaringan interkoneksi VPN L2TP/IPSec untuk mempermudah pada saat implementasi seperti pada gambar 3 di bawah ini.



Gambar 3. Rancangan Topologi VPN

b. Rancangan Pengujian *Delay*

Setelah dilakukan rancangan dan implementasi terkait penelitian ini, peneliti lanjut melakukan pengujian *delay* dan dibuatlah rancangan untuk mengukur *delay* seperti pada gambar 4 dibawah ini.

Metode	Ukuran Data	*Delay* (ms)
L2TP+IPSec		
L2TP+IPSec		
L2TP+IPSec		

Gambar 1. Rancangan Pengujian *Delay*

Untuk standarisasi pengukuran *delay* berdasarkan sumber Tiphon adalah sebagai berikut:

Tabel 1. Standarisasi Pengukuran *Delay*

Kategori Degradasi	*Delay*	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Buruk	> 450 ms	1

c. Rancangan Pengujian *Jitter*

Setelah pengukuran *delay*, selanjutnya peneliti juga merancang untuk pengujian *jitter* seperti pada gambar 5 di bawah ini.

Metode	Ukuran Data	*Jitter* (ms)
L2TP+IPSec		
L2TP+IPSec		
L2TP+IPSec		

Gambar 2. Rancangan Pengujian *Jitter*

Untuk standarisasi pengukuran *jitter* berdasarkan sumber Tiphon adalah sebagai berikut:

Tabel 2. Standarisasi Pengukuran *Jitter*

Kategori Degradasi	*Jitter*	Indeks
Sangat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	75 s/d 125 ms	2
Buruk	125 s/d 225 ms	1

d. Rancangan Pengujian *Packet Loss*

Setelah pengukuran *jitter*, selanjutnya peneliti juga merancang untuk pengujian *packet loss* seperti pada gambar 6 di bawah ini.

Metode	Ukuran Data	*Packet Loss* (%)
L2TP+IPSec		
L2TP+IPSec		
L2TP+IPSec		

Gambar 3. Rancangan Pengujian *Packet Loss*

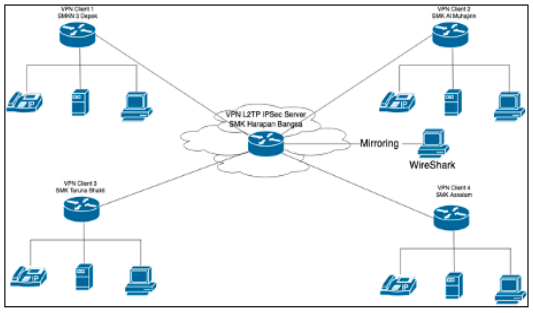
Untuk standarisasi pengukuran *packet loss* berdasarkan sumber Tiphon adalah sebagai berikut:

Tabel 3. Standarisasi Pengukuran *Packet Loss*

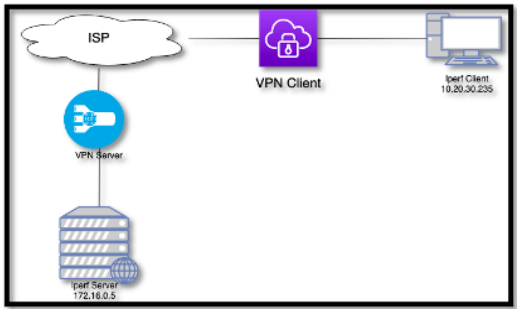
Kategori Degradasi	*Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Buruk	25 %	1

e. Rancangan Pengujian *Sniffing*

Setelah melakukan pengujian jaringan VPN dengan mengukur 3 parameter yaitu: *delay, jitter, packet loss.* Selanjutnya peneliti menguji keamanan jaringan VPN dengan teknik *sniffing* seperti pada rancangan gambar 7 dan 8 di bawah ini.



Gambar 4. Rancangan Pengujian Keamanan 1



Gambar 5. Rancangan Pengujian Keamanan 2

3.2 Hasil Penelitian

a. Hasil Pengujian *Delay*

Setelah dilakukan pengujian berdasarkan rancangan yang sudah dibuat untuk pengukuran *delay*, didapatkan hasil yang dinyatakan sangat bagus berdasarkan sumber Tiphon karena datanya menunjukan *delay* dibawah dari 150ms seperti pada gambar 9.

Metode	Ukuran Data	*Delay* (ms)
L2TP+IPSec	5 Mb	102.484 ms
L2TP+IPSec	10 Mb	140.283 ms
L2TP+IPSec	25 Mb	143.602 ms

Gambar 6. Hasil Pengujian *Delay*

b. Hasil Pengujian *Jitter*

Selanjutnya setelah mengukur nilai *delay*, dilanjutkan menguji nilai *jitter* dari rancangan yang sudah ditentukan, hasil yang didapat menurut standar Tiphon dinyatakan bagus karena nilai *jitter* dibawah 75ms seperti pada gambar 10.

Metode	Ukuran Data	Jitter (ms)
L2TP+IPSec	5 Mb	66.556 ms
L2TP+IPSec	10 Mb	66.557 ms
L2TP+IPSec	25 Mb	72.224 ms

Gambar 7. Hasil Pengujian *Jitter*

c. Hasil Pengujian *Packet Loss*

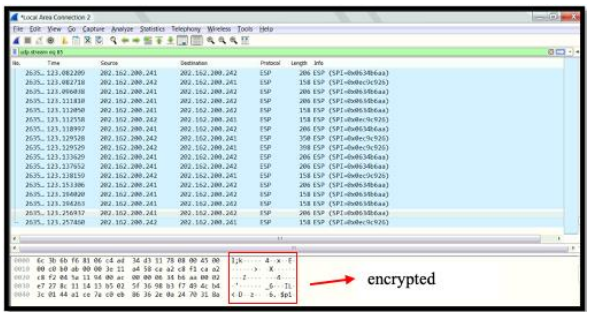
Selanjutnya setelah mengukur nilai *jitter*, dilanjutkan dengan menguji nilai *packet* loss dari rancangan yang sudah ditentukanm hasil yang didapat menurut standar Tiphon dinyatakan sangat bagus karena nilai *packet* loss tidak terjadi sama sekali atau 0% seperti pada gambar 11.

Metode	Ukuran Data	*Packet Loss* %
L2TP+IPSec	5 Mb	0%
L2TP+IPSec	10 Mb	0%
L2TP+IPSec	25 Mb	0%

Gambar 8. Hasil Pengujian *Packet Loss*

d. Hasil Pengujian *Sniffing*

Tahapan pengujian terakhir adalah menguji keamanan jaringan pada VPN L2TP/IPSec ini dengan sesuai rancangan yang sudah dituliskan. Hasil dari pengujian keamanan jaringan VPN ini dinyatakan cukup baik karena data yang melewati jaringan sudah terkenkripsi seperti pada gambar 12.



Gambar 9. Hasil Pengujian Keamanan Jaringan

4. KESIMPULAN

Dalam penelitian ini bertujuan untuk melakukan interkoneksi jaringan dengan menggunakan teknologi VPN L2TP/IPSec untuk menghubungkan antar sekolah TKJ Se-Depok. Setelah melakukan semua tahap dari analisis perancangan sampai ke implementasi dan pengujian, dapat ditarik kesimpulan untuk menjawab rumusan masalah pada penelitian ini ialah rancangan yang diimplementasikan terkait jaringan interkoneksi VPN menggunakan L2TP/IPSec dengan *routing* OSPF yang terkoneksi internet dapat berjalan dengan baik. Dan performa yang dihasilkan berdasarkan pengujian yang telah dilakukan juga mendapatkan hasil yang baik.

Adapun saran yang peneliti berikan untuk penelitian selanjutnya jika ingin melakukan penelitian yang serupa terkait interkoneksi jaringan VPN ini ialah peneliti selanjutnya dapat menggunakan protokol VPN selain L2TP/IPSec dalam melakukan penerapan atau implementasinya.

Ucapan Terima Kasih

Peneliti mengucapkan terima kasih kepada Sekolah Teknologi Terpadu Nurul Fikri, dan juga para guru yang tergabung dalam organisasi Musyawarah Guru Mata Pelajaran (MGMP) TKJ yang telah memberikan informasi, dukungan, dan juga masukan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. RACHMAWAN, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di atas VPN," *J. Manaj. Inform.*, vol. 8, no. 2, pp. 53–57, 2018

[2] I. I. R. D. A. M. K. Mila, "Perbandingan Tunneling VPN PPTP dan L2TP/IPSec pada Layanan VoIP di Politeknik Negeri Malang 1,2,3)," *J. JARTEL*, vol. Vol 6 No 1, no. ISSN 2407-0807, pp. 135–140, 2018, [Online]. Available: http://jtdjurnal.polinema.ac.id/index.php/jtd/ article/ view/74.

[3] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, "Analisis Perbandingan Performa QOS, PPTP, L2TP, SSTP dan IPSec pada Jaringan VPN Menggunakan Mikrotik," *semanTIK*, vol. 4, no. 2, pp. 29–36, 2018.

[4] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP," *J. Infotel*, vol. 9, no. 3, pp. 265–270, 2017, doi: 10.20895/infotel.v9i3.274.

[5] H. Sujadi and A. Burhanuddin, "Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode IPSEC VPN (Studi Kasus: Pt. Agrabudi Komunika)," *Infotech J.*, vol. 3, no. 2, p. 236702, 2017.

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

[7] P. Utomo and B. E. Purnama, "Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol *Routing Information Protokol* (RIP) dan Protokol *Open Shortest Path First* (OSPF)," *Indones. J. Netw. Secur.*, vol. 1, no. 1, pp. 8–25, 2012.

[8] D. Carol *et al.*, "Analisis Perbandingan Performa SSTP dan PPTP pada VPN 1Deona," pp. 1–15, 2017, [Online]. Available: journal.ukrim.ac.id/index.php/JFE/article/download/126/101.