RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer) Vol. 6 No. 1
e-ISSN : 2621-9700, p-ISSN : 2654-2684

Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (*Virtual Private Network*)

Muhammad Alvin Gunawan [1], Sukma Wardhana [2]
[1) 2)]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana
Jl. Raya Kranggan No.6, RT.006/RW.008, Jatiranggon, Kec. Jatisampurna, Kota Bekasi, Jawa Barat 17432
Email: [1)] 41518210048@student.mercubuana.ac.id, [2)] sukma@mercubuana.ac.id

ABSTRAK

VPN merupakan teknologi yang dapat membuat jaringan privat dengan memanfaatkan jaringan publik untuk mengamankan proses pertukaran data. Teknologi VPN biasanya digunakan untuk menghubungkan unit dan kantor cabang, yaitu dengan membangun terowongan antara dua lokasi. Penelitian ini memiliki tujuan utama untuk mengimplementasikan jaringan VPN antara cabang dan kantor cabang dengan penambahan jaringan keamanan untuk melindungi data agar tidak terkomunikasikan. Hal ini juga yang peneliti lakukan dalam makalah ini dengan membandingkan protokol VPN PPTP (Point-To-Point Tunneling Protocol) dan L2TP/IPsec (Layer Two Tunneling Protocol) menggunakan algoritma MPEE dan kunci enkripsi RSA RC4 128 untuk PPTP dan SHA -1 algoritma dengan AES 128 CBC, AES 128 CTR, enkripsi AES 128 GCM untuk protokol L2TP/IPsec. Setiap pengujian diberi beban lalu lintas unggah dan unduh sebesar 10MB, 20MB, dan 30MB. Hasil QoS (Quality of Service) yang meliputi throughput, packet loss, delay, dan jitter semuanya disajikan secara deskriptif dalam hasil penelitian ini. Kemudian dilakukan pengujian keamanan jaringan menggunakan Sniffing tanpa VPN, Sniffing PPTP, dan Sniffing L2TP. Pengujian keamanan jaringan menunjukkan bahwa data telah berhasil dienkripsi karena dalam pengujian keamanan ini Anda juga melihat aspek kerahasiaan apakah sudah terpenuhi atau belum.

Kata Kunci: VPN; PPTP; L2TP/IPsec; Quality of Service; Security

ABSTRACT

VPN is a technology that can create a private network by utilizing public network so that the data exchange process becomes secure. VPN technology is typically used to connect the unit and Branch offices, namely by constructing a tunnel between the two locations. This research has the main objective of implementing a VPN network between Branches and Branch offices with the addition of a security network to protect the data to be communicated. This is also what the researchers did in this paper by comparing the VPN protocols PPTP (Point-To-Point Tunnelling Protocol) and L2TP/IPsec (Layer Two Tunnelling Protocol) using the MPEE Algorithm and RSA RC4 encryption key 128 for PPTP and the SHA-1 Algorithm with AES 128 CBC, AES 128 CTR, AES 128 GCM encryption for L2TP/IPsec protocol. Each test is assigned upload and download traffic loads of 10MB, 20MB and 30MB. The QoS (Quality of Service) results including throughput, packet loss, delay, jitter all presented descriptively in the results of this study. Then the network security test is performed using Sniffing without VPN, PPTP Sniffing and L2TP Sniffing. The network security test shows that the data has been successfully encrypted because in this security test you also see the confidentiality aspect whether it has been met or not.

Keywords: VPN; PPTP; L2TP/IPsec; Quality of service; Security

1 PENDAHULUAN

Kebutuhan akan pengetahuan semakin berkembang seiring dengan berkembangnya teknologi informasi saat ini. Ketika setiap orang membutuhkan informasi dengan cepat, kemajuan yang cepat dapat memiliki efek menguntungkan dan negatif pada tantangan keamanan, seperti pencurian data. Efek positif termasuk mempercepat pencarian informasi. Jalannya operasional suatu organisasi atau lembaga tidak akan lepas dari berbagi informasi di antara para pemangku kepentingannya [1].

Pembuatan VPN merupakan salah satu cara untuk meningkatkan keamanan data pada jaringan komputer (*Virtual Private Network*) VPN dapat mengirimkan data pengguna melalui layanan jaringan publik yang murah, terutama melalui *internet*. Hal ini tidak terlepas dari penggunaan jaringan *internet* yang dapat saling terhubung satu sama lain [2]. VPN lebih terjangkau daripada jaringan pribadi yang tradisional, itulah sebabnya banyak bisnis dan penyedia telekomunikasi menggunakan VPN [3]. Keuntungan utama VPN dari sudut pandang konsumen adalah biaya yang cukup terjangkau. *Tunneling*

berkecepatan tinggi adalah jawaban untuk menggunakan teknologi VPN. *Tunneling* seperti itu yang mahal dan menantang untuk dipelihara, serta menantang untuk dikendalikan. Pengguna layanan VPN dapat mengandalkan *internet*. Modem *dial-up* memungkinkan akses ke *internet* bahkan dari tempat yang paling terpencil sekalipun. Pengguna *dial-in* dapat berkomunikasi dengan aman berkat VPN. VPN menerima layanan akurat dari *internet*. Satu-satunya pilihan untuk menghubungkan pengguna ponsel ke situs perusahaan ketika *leased line* tidak tersedia adalah dengan menggunakan teknologi VPN [4].

Keamanan *software* perlu dievaluasi dan dikendalikan pada tingkat yang dapat dikelola mengingat penggunaan *software* VPN yang meluas di sektor bisnis saat ini. Pengguna dapat dengan aman terhubung dari jarak jauh ke jaringan bahkan jika mereka secara fisik berada di luar melalui VPN. VPN yang pada dasarnya adalah terowongan pribadi terenkripsi melalui jaringan [5]. VPN masih terus diteliti dan dieksplorasi sebagai *software* yang terus berkembang [6].

Sejumlah besar data yang dikumpulkan dan dihasilkan setiap hari menawarkan berbagai peluang analitis bagi organisasi untuk mengungkap informasi yang berguna untuk operasi mereka [7]. Keamanan data dalam suatu jaringan dapat ditingkatkan dengan menerapkan keamanan VPN. Alih-alih menggunakan jalur sewaan atau jalur eksklusif dari penyedia, bisnis memilih untuk menggunakan VPN. VPN menawarkan fitur keamanan seperti enkripsi dan otentifikasi dan lebih hemat biaya [8]. Setiap aplikasi VPN yang efektif dapat dibandingkan dalam hal pengoptimalan di antara banyak aplikasi VPN. Izin dan pengaturan VPN yang sama dengan jaringan lokal juga dapat digunakan untuk melakukannya di jaringan publik. Dua protokol *tunneling* yang dapat digunakan dengan VPN adalah *Point-to-Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP) [9]. Karena ada beberapa *server* VPN yang ada di VPN yang besar dan rumit, topologi jaringan tentu akan berdampak pada kinerja VPN. Solusi jaringan alternatif akan menawarkan berbagai *Quality of Service* (QoS), sehingga penting untuk menyelidiki apakah topologi jaringan VPN yang berbeda berpengaruh pada kinerja [10].

Memanfaatkan VPN memiliki efek positif pada perlindungan privasi koneksi jaringan. Ketika berbagai tugas jaringan dilakukan melalui koneksi pribadi ini, masalah muncul kembali [11]. Dengan menggunakan PPTP dan L2TP/IPsec, makalah ini bermaksud untuk membuat dan mengevaluasi kinerja VPN berdasarkan perbedaan antara kedua protokol tersebut. Dua protokol VPN yang berbeda ditawarkan untuk menilai kinerja dan menyelidiki hubungan antara kinerja VPN dan topologi yang direncanakan dengan membuat metrik kinerja jaringan VPN secara metodis. Mengikuti implementasi kedua protokol ini, hasil *throughput, packet loss, delay,* dan *jitter* dari analisis *Quality of Service* (QoS) diperiksa. *Quality of Service* (QoS) merupakan tantangan berkelanjutan di industri telekomunikasi, terutama karena berdampak pada penyediaan layanan telekomunikasi [12]. Selanjutnya, PPTP, L2TP/IPsec dan tidak ada VPN yang terdeteksi untuk memeriksa keamanan jaringan. Untuk meningkatkan kualitas dan keamanan layanan VPN, pekerjaan ini dapat digunakan untuk menerapkan sistem VPN dalam praktiknya.

2 TINJAUAN PUSTAKA

Pada bagian ini, kami memberikan informasi latar belakang untuk membuat makalah ini lebih lengkap dan mandiri. Di sisa bagian ini, kami secara singkat mendefinisikan jaringan komputer dan VPN. Setelah itu, kami memberikan definisi komponen jaringan yang digunakan dalam VPN. Kami kemudian memberikan bagian latar belakang teknis yang membahas secara singkat protokol yang digunakan dalam solusi dan teknologi VPN seluler. Kami menyimpulkan bagian dengan diskusi tentang klasifikasi VPN untuk kelengkapan.

Jaringan komputer adalah kumpulan komputer yang terhubung, printer, dan peralatan lainnya. Informasi dan data bergerak melalui kabel, memungkinkan pengguna jaringan komputer untuk bertukar dokumen dan data, mencetak ke printer yang sama, dan berbagi perangkat keras atau perangkat lunak jaringan [13].

Untuk membangun jaringan komputer, *router* dan *switch* digunakan dalam berbagai protokol dan algoritma untuk dapat bertukar data/informasi dan mengangkut data ke titik akhir yang diinginkan. Setiap titik akhir pada jaringan memiliki pengidentifikasi unik.

Berdasarkan wilayah yang dapat dijangkau atau dilayani, jaringan komputer dapat dikelompokkan menjadi tiga jenis, yaitu LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), dan WAN (*Wide Area Network*).

LAN (*Local Area Network*) adalah salah satu jenis jaringan informasi yang paling penting untuk menyediakan komunikasi di komunitas terbatas seperti universitas dan institusi. LAN terdiri dari sekelompok komputer yang saling berhubungan dan perangkat komunikasi lainnya, yang terhubung satu sama lain melalui sistem rekayasa terintegrasi. Mereka didistribusikan di wilayah geografis yang relatif kecil dan dicirikan oleh komunikasi berkecepatan tinggi dan bebas kesalahan. Dengan

demikian, jaringan area lokal adalah campuran perangkat, peralatan, dan institusi yang saling terkait, di mana mereka membentuk struktur yang disebut jaringan. Jaringan ini terutama didasarkan pada komponen fisik dan perangkat lunak penting untuk beroperasi secara efisien [15].

MAN (*Metropolitan Area Network*) adalah konsep jaringan komputer yang menggunakan kabel atau nirkabel dan berlaku untuk area seluas kota. MAN dapat Mengelola koneksi komputasi hingga 10 km [16]. Jika diterapkan dalam satu kawasan, maksimal yang bisa dikelola mencapai luas 100 Km^2. Contoh penerapan jaringan MAN adalah penyedia infrastruktur jaringan atau ISP yang menyediakan layanan informasi dan komunikasi bagi konsumen. Atau bisa juga berupa layanan radio yang dapat diakses oleh pendengar di suatu wilayah kota [17].

WAN (*Wide Area Network*) adalah kumpulan jaringan. WAN memungkinkan dua pengguna atau sistem pada LAN yang berbeda untuk berkomunikasi atau bertukar data. WAN menjangkau bermil-mil dan menyediakan layanan di wilayah geografis yang sangat luas. WAN menggunakan perangkat, sistem, dan media yang tidak dapat digunakan di LAN. WAN berbeda dari LAN dalam hal protokol, perangkat, teknologi, dan media[18].

VPN (*Virtual Private Network*) sendiri merupakan teknologi komunikasi yang memungkinkan Anda untuk terhubung ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal [19]. Dalam pengertian lain, VPN juga berarti suatu teknik keamanan jaringan yang bekerja dengan cara membuat *tunnel* bagi jaringan yang terpercaya untuk menghubungkan jaringan yang ada di luar negeri melalui *Internet*. Dalam teknologi VPN, protokol keamanan yang paling umum digunakan untuk mengamankan koneksi [20]. VPN juga merupakan jaringan pribadi virtual dan logis, yang menciptakan jaringan pribadi virtual melalui *Internet* dan melakukan komunikasi terenkripsi [21].

VPN pada awalnya dirancang untuk membangun konektivitas ke jaringan pribadi jarak jauh dan mengakses layanan jarak jauh mereka. Saat ini, mereka terutama digunakan untuk penjelajahan yang ramah privasi: tujuan mereka adalah untuk menutupi alamat IP sumber asli dengan titik akhir VPN dan dengan demikian melindungi penggunanya agar tidak dipantau oleh penyedia, misalnya. Penyedia Layanan *Internet* (ISP). Untuk kasus penggunaan itu, sangat penting bahwa semua lalu lintas diarahkan melalui terowongan VPN dan tidak ada yang bocor ke jaringan perantara selain dari koneksi VPN itu sendiri [22]. Program yang berjalan pada VPN akan mendapat manfaat dari efisiensi, perlindungan, dan arah jaringan pribadi Anda [23].

Beberapa protokol yang digunakan untuk pengembangan VPN adalah sebagai berikut [24]:

- PPTP (Point to Point Tunnelling Protocol)
- L2TP (Layer Two Tunnelling Protocol)
- IPsec (Internet Protocol Security)
- PPTP over L2TP
- IP-in-IP

Protokol VPN diklasifikasikan ke dalam situs-ke-situs dan VPN akses jarak jauh, yang menunjukkan serangkaian fitur yang berbeda dalam hal mekanisme keamanan [26]. Untuk mencapai hal tersebut digunakan VPN yang menggunakan beberapa protokol yang aman [27].

Bagian ini akan menyajikan secara singkat berbagai protokol yang menjadi dasar dari solusi VPN yang dibahas pada hasil dan pembahasan.

PPTP adalah protokol jaringan yang memungkinkan transfer data secara aman melalui klien jarak jauh (klien jauh dari *server*) ke *server* pribadi perusahaan dengan membangun VPN melalui TCP/IP [28]. PPTP dapat mengubah paket PPP menjadi datagram IP sehingga dapat ditransmisikan melalui *Internet*. Protokol ini dikembangkan oleh *Microsoft* dan *Cisco*. Teknologi *tunnel*ing PPTP merupakan perpanjangan dari *Point-to-Point Remote Access Protocol* yang dikeluarkan oleh *Internet Engineers Task Force* (ITEF) [29]. Tahapan dalam membangun sistem VPN menggunakan PPTP berbasis *proxy* adalah [30]:

- Kebutuhan inventaris;
- Analisis dan desain sistem jaringan;
- Pelaksanaan; dan
- Pengujian.

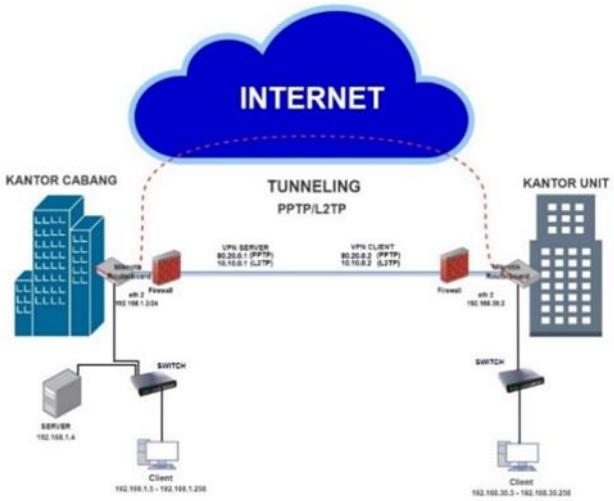
L2TP merupakan hasil pengembangan dari protokol PPTP plus L2F. Protokol keamanan jaringan dan enkripsi yang digunakan untuk otentikasi sama dengan PPTP. Namun, untuk melakukan panggilan/komunikasi, L2TP menggunakan UDP port 1701. L2TP sering digunakan untuk membuat virtual private network (VPN) yang terletak di jaringan publik, seperti *Internet* [31]. L2TP lebih "ramah firewall" daripada jenis VPN lain seperti PPTP. Ini adalah keuntungan besar jika Anda menggunakan protokol ini, karena kebanyakan firewall tidak mendukung GRE. Namun, L2TP tidak memiliki enkripsi, sehingga kami membutuhkan layanan tambahan untuk mendukung keamanan yang lebih tinggi [32].

IPsec dikenal sebagai Keamanan IP. Dalam IPsec, paket data yang dikirim melalui L2TP VPN dapat dienkapsulasi lebih lanjut untuk membuat komunikasi antara *server* dan klien lebih aman. Ada proteksi ganda dalam keamanan jaringan: proteksi pertama menciptakan koneksi *Point-to-Point*

Protocol (PPP) antar pengirim, sedangkan proteksi kedua adalah enkripsi untuk keamanan yang memanfaatkan IPsec [33].

3 METODOLOGI

Disarankan pendekatan *Virtual Private Network* (VPN), Alamat IP setiap komponen jaringan dilindungi oleh mikrotik. Dalam hal ini mikrotik akan mengamankan unit dan kantor cabang yang telah diuji pada router mikrotik, digunakan dalam rencana jaringan yang diusulkan untuk menghubungkan kantor cabang dan unit. Router kantor cabang bertindak sebagai *server* PPTP dan L2TP, sedangkan router kantor unit bertindak sebagai klien PPTP dan L2TP. Keduanya kemudian dapat berbagi info.



Gambar 1 Topologi jaringan.

Tabel 1. IP Address

Devices	***IP Address***	***Subnet***
ISP (*Branch*)	192.168.100.4	255.255.255.0
ISP (Unit)	192.168.100.2	255.255.255.0
PPTP *Tunnel* Router *Branch*	80.20.0.1	255.255.255.0
L2TP/IPsec *Tunnel* Router *Branch*	10.10.0.1	255.255.255.0
PPTP *Tunnel* Router Unit	80.20.0.2	255.255.255.0
L2TP/IPsec *Tunnel* Router Unit	10.10.0.2	255.255.255.0
File Server	192.168.1.4	255.255.255.0
Client Branch Office	192/168.1.5 s/d 254	255.255.255.0
Client Unit *Office*	192/168.30.3 s/d 254	255.255.255.0

Tabel 2 Kebutuhan *Software* dan *Hardware.*

Item	***Item Name***	***Specification***
PC		*AMD Ryzen 5 1600 Six-Core CPU 3.20GHz RAM 8 GB Windows 10Pro 64-Bit.*
Laptop	*HP 14S DK1002AU*	*AMD Athlon Silver 3050U with Radeon Graphics 2.30 GHz RAM 4,00 GB Windows11 64-Bit.*
Mikrotik	*Router Board RB9541Ui-2HnD*	*Architecture MIPS-BE CPU AR9344 600 MHz RAM 128 MB*
Aplikasi	*Win box Wireshark FileZilla Draw.io*	

Mengikuti topologi jaringan pada tabel 1, pengujian *tunneling* VPN dilakukan menggunakan perangkat lunak *File zilla*.

Untuk mengimplementasikan VPN, setiap *tunnel* PPTP dan L2TP/IPsec memerlukan konfigurasi setiap metode yang sesuai dengan kondisi. Ini adalah langkah-langkah konfigurasi:

1. Konfigurasikan *server* cabang mikrotik
a. Konfigurasi *Router* pengguna
b. Mengatur alamat IP *router*
c. Cabang *Router* DNS Statis
d. Cabang *Router* Statis *Gateway*
2. Pengaturan unit klien mikrotik
a. Konfigurasi *router* pengguna
b. Mengatur alamat IP *router*
c. Unit Router Statis DNS
d. Unit Router Statis *Gateway*
3. Konfigurasi *Tunnel* PPTP Kantor Cabang
4. Konfigurasi *tunnel* unit PPTP
5. Konfigurasi cabang L2TP/IPsec
6. Konfigurasi unit L2TP/IPsec

Kebutuhan *software* dan *hardware* dalam perancangan jaringan dapat dilihat pada tabel 2 di bawah ini.

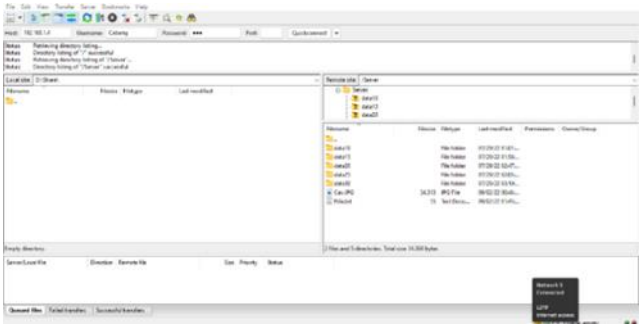
Tahap pengujian ini mengeksekusi hasil konfigurasi yang diperoleh melalui metode PPTP dan L2TP/IPsec. Dalam pengujian PPTP, algoritma RSA digunakan dengan enkripsi RC4. Selanjutnya, untuk pengujian L2TP/IPsec digunakan algoritma SHA-1 dengan enkripsi AES 128 CBC, AES 128 CTR, AES 128 GCM, dan Camelia 128. Tes unggah dan unduh adalah 10MB, 20MB, dan 30MB untuk hasil *Quality of Service* (QOS), yang meliputi *throughput, packet loss, delay, jitter*.

Tahap akhir pengujian adalah pengujian performansi jaringan VPN PPTP dan L2TP/IPsec yang telah selesai dilakukan sehingga dapat dilihat hasilnya. Pengujian enkripsi pada VPN PPTP dilakukan dengan cara observasi (PPP kompresi data) dan untuk L2TP/IPsec dilakukan dengan cara observasi (*Encapsulating Security Payload*). Pengamatan dilakukan untuk mengetahui apakah paket data data tersebut telah dienkripsi atau belum untuk mengetahui terpenuhi atau tidaknya aspek kerahasiaan.

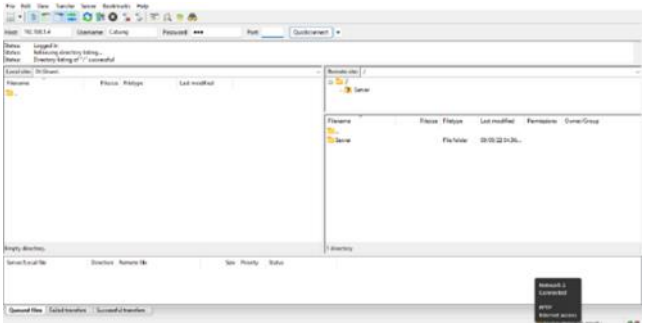
4 HASIL DAN PEMBAHASAN

Pengujian *tunneling* VPN digunakan untuk transfer data antar Cabang dan Unit menggunakan *File zilla* dengan tujuan untuk membandingkan *Quality of Service* (QoS) dari kedua metode yang digunakan. Tes ini melibatkan pengunduhan 5 *file* dengan berbagai ukuran menggunakan protokol PPTP dan L2TP/IPsec.

Setelah terhubung ke klien PPTP dan L2TP, luncurkan *File Zilla* dan masuk dengan nama pengguna dan kata sandi. Alamat IP *Server* untuk penyetelan PPTP dan L2TP/IPsec adalah 192.168.1.4, Nama Pengguna adalah Cabang, dan Kata Sandi adalah 123.



Gambar 2 Login *File zilla* PPTP



Gambar 3 Login *File zilla* L2TP

A. Analisis Quality of Service (QoS)

1) Uji PPTP

Pada hasil QoS PPTP menggunakan masing-masing beban trafik 10 MB, 20 MB dan 30 MB didapatkan hasil sebagai berikut:

a) 10 MB Upload
1. *Througput*
   a. RC4 *Algorithm*: 5.34
   2. *Packet loss*
   a. RC4 *Algorithm*: 0%
   3. *Delay*
   a. RC4 *Algorithm*: 190.7
   4. *Jitter*
   a. RC4 *Algorithm*: 144.2

b) 10 MB Download
1. *Througput*
   a. RC4 *Algorithm*: 5.25
2. *Packet loss*
   a. RC4 *Algorithm*: 0%
3. *Delay*
   a. RC4 *Algorithm*: 146.2
4. *Jitter*
   a. RC4 *Algorithm*: 146.5

c) 20 MB Upload
1. *Througput*
   a. RC4 *Algorithm*: 8.164
2. *Packet loss*
   a. RC4 *Algorithm*: 0%
3. *Delay*
   a. RC4 *Algorithm*: 101.1
4. *Jitter*
   a. RC4 *Algorithm*: 782.3

d) 20 MB Download
1. *Througput*
   a. RC4 *Algorithm*: 8.71
2. *Packet loss*
   a. RC4 *Algorithm*: 0%

3. *Delay*
   a. RC4 *Algorithm*: 931.7
4. *Jitter*
   a. RC4 *Algorithm*: 929.5

e) 30 MB Upload

1. *Througput*
   a. RC4 *Algorithm*: 10
2. *Packet loss*
   a. RC4 *Algorithm*: 0%
3. *Delay*
   a. RC4 *Algorithm*: 812.7
4. *Jitter*
   a. RC4 *Algorithm*: 818.5

f) 30 MB Download

1. *Througput*
   a. RC4 *Algorithm*: 7.29
2. *Packet loss*
   a. RC4 *Algorithm*: 0%
3. *Delay*
   a. RC4 *Algorithm*: 112.1
4. *Jitter*
   a. RC4 *Algorithm*: 111.7

2) Uji L2TP

Pada hasil QoS L2TP/IPsec menggunakan masing-masing beban trafik 10 MB, 20 MB dan 30 MB, hasilnya adalah sebagai berikut:

a) 10 MB Upload

1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 3.741
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 5.623
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 4.974
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 4.52
2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 178.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 145.9
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 134.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 182.2
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 177.6
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 144.5
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 132.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 167.9

b) 10 MB Download

1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 131.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 952.2
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 112.3
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 112
2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 109.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 243.1
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 161.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 111.5
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 109.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 262.7
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 160.4
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 111.4

c) 20 MB Upload

1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 6.168
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 8.647
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 7.358
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 6.803
2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 131.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 952.2
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 112.3
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 112
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 131.8
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 893
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 111.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 112.2

d) 20 MB Download

1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 7.282
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 6.541
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 9.034
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 7.927

2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 108.9
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 123
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 891.95
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 298.4
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 108.7
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 119.4
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 866.63
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 318.4

e) 30 MB Upload

1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 2.287
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 6.947
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 8.101
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 7.794
2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 364.4
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 119.6
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 102.6
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 102.2
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 366.1
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 121.3
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 873
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 102.1

f) 30 MB Download

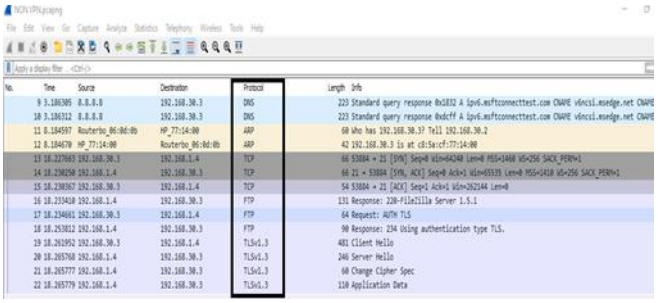
1. *Througput*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 7.248
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 9.155
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 8.019
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 8.232
2. *Packet loss*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 0%
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 0%
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 0%
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 0%
3. *Delay*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 111.5
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 891.7
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 101.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 947.4
4. *Jitter*
   a. AES 128 CBC (SHA-1 *auth*) *Algorithm*: 111.4
   b. AES 128 CTR (SHA-1 *auth*) *Algorithm*: 873.5
   c. AES 128 GCM (SHA-1 *auth*) *Algorithm*: 103.8
   d. Camelia 128 (SHA-1 *auth*) *Algorithm*: 948.7

A. Uji Keamanan Jaringan

Pengujian keamanan jaringan dilakukan dalam tiga konfigurasi dalam penelitian ini: pengujian jaringan tanpa VPN, pengujian jaringan dengan PPTP VPN, dan pengujian jaringan dengan VPN L2TP/IPsec menggunakan *Wireshark*.

1) Hasil *Sniffing* Non-VPN

Setelah menginstal perangkat lunak *Wireshark* pada klien, klien menangkap jaringan yang melewati setiap paket data untuk diendus oleh *wireshark*. *Sniffing* akan mengungkapkan data yang dikirim dari klien ke *server*. Isi paket kemudian akan dianalisis untuk mengidentifikasi celah keamanan jaringan saat menerima dan mengirim data.



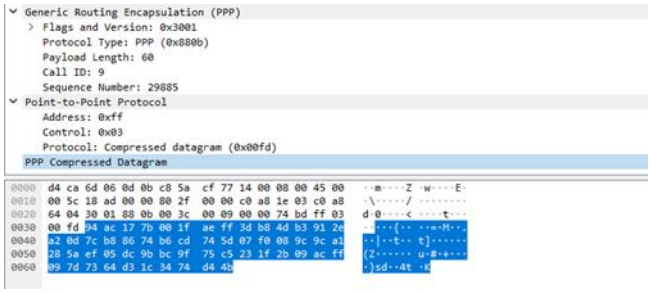
Gambar 4 Hasil *Sniffing* Non VPN

Hasil *Sniffing* pada Gambar 4 dapat dilihat pada beberapa protokol lain seperti: DNS, ARP, TCP, FTP, TLS. Data menunjukkan bahwa sumber adalah alamat asal sedangkan tujuan menunjukkan alamat tujuan. IP *Server* FTP adalah (192.168.1.4) Meskipun ada TLSV 1.3 (*Transport Layer Security* Versi 1.3) di *File zilla*, IP *Address Server* masih terlihat karena tidak ada enkripsi pada paket data.

2) Hasil *Sniffing* VPN PPTP

Berdasarkan pengujian jaringan VPN PPTP juga dilakukan *Sniffing* yaitu menangkap paket data yang lewat antara *server* dan *client* dalam jaringan VPN,

hasil pengujian keamanan jaringan VPN PPTP adalah sebagai berikut pada gambar 5.



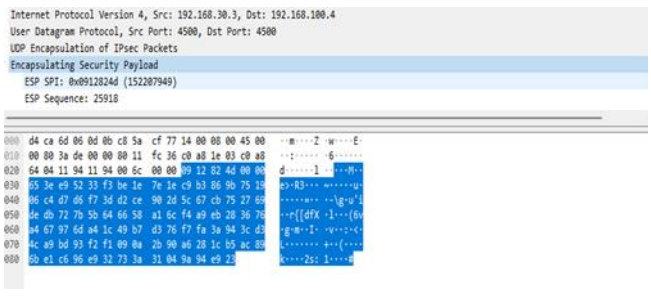
Gambar 5 Hasil *Sniffing* VPN PPTP

IP FTP yang digunakan untuk berkomunikasi antara *server* dan klien tidak terlihat karena IP pada FTP telah dienkripsi dengan PPTP. Saat berkomunikasi antara Klien dan *Server*, TCP digunakan, dan GRE dienkapsulasi dengan PPP selama koneksi antara klien PPTP (192.168.30.2) dan *Server* PPTP (192.168.100.4). Klien kemudian mengirimkan pesan Pengakuan ke *server*, yang menunjukkan bahwa persetujuan klien telah menerima koneksi.

Enkripsi kinerja PPTP VPN kemudian diuji dengan mengamati pengambilan paket data terkompresi. Ini menunjukkan bahwa paket data dienkripsi dan dienkapsulasi dalam datagram IP yang berisi paket PPP. Datagram IP dihasilkan dengan memodifikasi protokol *Internet Generic Routing Encapsulation* (GRE). PPP Frames berisi PPP Header, IP Header, TCP Header, dan Data.

3) Hasil *Sniffing* VPN L2TP/IPsec

Pengujian terakhir adalah *Sniffing* dengan VPN L2TP/IPsec, yang bertujuan untuk meningkatkan tingkat keamanan paket data yang dilewati dengan hasil sebagai berikut pada gambar 6. Data Enkripsi Protokol IPsec yang dikirim antara klien dan *server* IP pada FTP telah dienkripsi dengan L2TP/IPsec VPN, seperti yang ditunjukkan pada Gambar 6. Protokol yang digunakan saat berkomunikasi antara *Client* dan *Server* adalah TCP, ESP Informasi yang terkandung dalam pesan *signaling* tidak dapat diketahui karena telah dienkapsulasi oleh header ESP.



Gambar 6 Hasil *Sniffing* VPN L2TP.

5 KESIMPULAN

Sesuai dengan penjelasan di atas, VPN *tunnel*ing harus dibangun terlebih dahulu untuk membangun *server* antar cabang dan unit. *Tunnel*ing VPN harus dibangun untuk menentukan hasil QoS masing-masing protokol. Selanjutnya dianalisis QoS untuk upload dan download menggunakan beban 10 MB, 20 MB dan 30 MB. Dari hasil tersebut penulis mendapatkan QOS sebagai data deskriptif yang disajikan dalam bentuk throughput, *packet loss*, *delay*, dan *jitter*. Setelah hasil QoS diterima, keamanan jaringan diuji untuk memastikan bahwa paket data telah dienkripsi dengan benar dan aspek kerahasiaan terpenuhi atau tidak. Pengamatan juga dilakukan untuk mengetahui apakah data paket data tersebut dienkripsi atau tidak.

DAFTAR PUSTAKA

[1] 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.

[2] Sumarna and A. Maulana, "Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta," *Expert J. Manaj. Sist. Inf. dan Teknol.*, vol. 11, no. 2, p. 90, 2021, doi: 10.36448/expert.v11i2.1829.

[3] Y. Zhou, "DoS Vulnerability Verification of IPSec VPN," *Proceedings of 2020 IEEE International Conference on Artificial Intelligence and Computer Applications, ICAICA 2020*. pp. 698–702, 2020, doi: 10.1109/ICAICA50127.2020.9182437.

[4] D. Y. K. Sharma* and C. Kaur, "The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2336–2339, 2020, doi: 10.35940/ijrte.f8335.038620.

[5] J. Jones, "PPTP VPN: An Analysis of the Effects of a DDoS Attack," *Conference Proceedings - IEEE SOUTHEASTCON*, vol. 2019. 2019, doi: 10.1109/SoutheastCon42311.2019.9020514.

[6] W. K. He, Z. Peng, C. W. Chao, Z. X. Kang, and C. A. Jun, "Tunneling SSL VPN Based on PF _ RING," pp. 3–6, 2019.

[7] Z. Munawar and N. I. Putri, "KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[8] A. Alshalan, S. Pisharody, and D. Huang, "A Survey of Mobile VPN Technologies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016, doi: 10.1109/COMST.2015.2496624.

[9] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus : Dinhubkominfo Kabupaten Banyumas)," *J. Infotel*, vol. 9, no. 3, pp. 265–270, 2017.

[10] Z. Wu and M. Xiao, "Performance evaluation of VPN with different network topologies," *2019 2nd Int. Conf. Electron. Technol. ICET 2019*, pp. 51–55, 2019, doi: 10.1109/ELTECH.2019.8839611.

[11] Z. Nagy and M. K. Wali, "Virtual private network impacts on the computer network performance with different traffic generators," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 881, no. 1, 2020, doi: 10.1088/1757-899X/881/1/012126.

[12] J. A. Caicedo-Muñoz, A. Ledezma Espino, J. C. Corrales, and A. Rendón, "QoS-Classifier for VPN and Non-VPN traffic based on time-related features," *Comput. Networks*, vol. 144, pp. 271–279, 2018, doi: 10.1016/j.comnet.2018.08.008.

[13] S. I. Jaya, R. Efendi, and N. Miyono, "Pemanfaatan Point-to-Point Tunneling Protocol (PPTP) pada Virtual Private Network dalam Akses File Server," *Teknol. Inf. - Aiti*, vol. 9, no. 2, pp. 101–200, 2013.

[14] N. K. Dewi and A. S. Putra, "Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT . ARS Solusi Utama)," *TEKINFO*, vol. 22, no. 1, pp. 66–81, 2021.

[15] Y. M. M. Al Sawy, "Components and means of communication within the Local Area Network: An analytical study," *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 3, pp. 74–81, 2018.

[16] Nugroho;Alhamri;Cinderatama, "Instalasai Jaringan Metropolitan Area Network (MAN) di 46 Kelurahan Kota Kediri," *J. Ilmu Pengetah. dan Teknol. Terintegrasi*, vol. 2, no. 2, pp. 69–75, 2018.

[17] R. Khasawneh, R. Alrifai, and H. Abusalem, "Wide Area Networks: a Comparison of Different Approaches for Hands-on Labs," *Issues Inf. Syst.*, vol. 4, pp. 191–197, 2013.

[18] S. Sudirman, S. Sumarsono, and A. S. Honggowibowo, "Perancangan Aplikasi Manajemen Peralatan Jaringan Komputer," *Compiler*, vol. 2, no. 1, 2013, doi: 10.28989/compiler.v2i1.41.

[19] A. Rachmawan and A. Prihanto, "Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet di Atas VPN," *J. Manaj. Inform.*, vol. 8, no. 2, pp. 53–57, 2018.

[20] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid End-to-End VPN Security Approach for Smart IoT Objects," *J. Netw. Comput. Appl.*, vol. 158, no. January 2018, p. 102598, 2020, doi: 10.1016/j.jnca.2020.102598.

[21] S. Liu, "Application of VPN Based on L2TP and User's Access Rights in Campus Network," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10989. pp. 676–686, 2018, doi: 10.1007/978-3-030-00563-4_66.

[22] C. Burkert, "Analysing Leakage during VPN Establishment in Public Wi-Fi Networks," *IEEE International Conference on Communications*. 2021, doi: 10.1109/ICC42927.2021.9500375.

[23] J. R. Raj and S. Srinivasulu, "Design of IoT Based VPN Gateway for Home Network," *Proc. Int. Conf. Electron. Renew. Syst. ICEARS 2022*, no. Icears, pp. 561–564, 2022, doi: 10.1109/ICEARS53579.2022.9751838.

[24] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[25] J. Gunawan and H. Agung, "IMPLEMENTATION OF PPTP AND BCP WITH INTER- VLAN ON THE TOPOLOGY THAT USES 2 ISP AS INTER-DIVISION CONNECTORS (Case Study: PT Kenari Djaja Prima)," *J. Algoritm. Log. dan Komputasi*, vol. 2, no. 1, pp. 138–150, 2019, doi: 10.30813/j-alu.v2i1.1574.

[26] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, pp. 39–44, 2017, doi: 10.1109/NSysS.2017.7885799.

[27] D. Rybin, "Investigation of the applicability of SSL/TLS protocol for VPN in APCS," *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, vol. 2018. pp. 1318–1321, 2018, doi: 10.1109/EIConRus.2018.8317339.

[28] M. Arafah and A. Gunawan, "Perancangan dan Simulasi Penerapan Virtual Private Network Menggunakan Metode PPTP (Studi Kasus Pada PT Pelindo IV Makassar)," *Inspir. J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, pp. 155–160, 2017, doi: 10.35585/inspir.v7i2.2450.

[29] 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.

[30] I. Ekawati and D. Irwan, "Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik," *JREC (Journal Electr. Electron. ISSN*, vol. 9, no. 1, pp. 29–40, 2021.

[31] N. E. Pamungkas, "Analisis Perbandingan Kinerja PPTP dan L2TP Pada Layanan Voice Over IP (VoIP)," no. 672015263, 2019.

[32] 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. Unsrat*, vol. 11, no. 1, p. 143279, 2017.

[33] J. Safira, Hanafi, and Munawar, "IMPLEMENTASI JARINGAN VPN L2TP / IPSEC MENGGUNAKAN LINUX DI LABORATURIUM JARINGAN KOMPUTER," *J. TEKTRO*, vol. 5, no. 1, pp. 59–63, 2021.