



JCSAI

Journal of Computation Science And Artificial Intelligence



Journal homepage:

<https://jcsai.xjournal.com/index.php/journal/index>

e-ISSN: 3032-4653

Vol. 2, No. 1, 2025

IMPLEMENTASI JARINGAN VPN METODE L2TP SEBAGAI JARINGAN PENUNJANG PEKERJA LAPANGAN PT ALBANY CORONA LESTARI CABANG CIREBON

Apan Apriyadi¹, Faisal Akbar², Mukidin³

Sekolah Tinggi Ilmu Komputer Poltek Cirebon

¹apriyadi.apan@gmail.com, ²faisal.akbar@stikompoltek.ac.id, ³mukidin@stikompoltek.ac.id

Abstrak

PT Albany Corona Lestari merupakan anak perusahaan dari PT Indomarco PrismaTama yang berfokus pada support toko Indomaret dalam hal kelistrikan, jaringan, perangkat keras, dan pelatihan karyawan toko. PT Albany Corona Lestari memiliki pekerja di kantor dan lapangan. Dalam bekerja, pekerja lapangan berpatokan pada website Complaint Online untuk memeriksa daftar komplain yang masuk, dan ESS (*Employee Self Service*) untuk absen, input izin, dan cuti. Permasalahan dalam akses ke website Complain Online dan ESS menjadi penghambat dalam bekerja, karena website hanya tersedia dalam jaringan lokal kantor dan jaringan lokal toko Indomaret, sehingga tidak dapat diakses melalui jaringan publik (internet). Masalah tersebut dapat diatasi dengan menggunakan VPN (*Virtual Private Network*) agar perangkat pekerja lapangan seperti laptop dan smartphone dapat mengakses jaringan lokal kantor dan membuka website Complaint Online dan ESS (*Employee Self Service*) dari mana saja dan kapan saja. VPN yang digunakan pada penelitian ini adalah L2TP (*Layer 2 Tunneling Protocol*) dengan ditambah IPSec (*Internet Protocol Security*) sebagai keamanan tambahan. Jaringan VPN L2TP yang telah terpasang dianalisa dengan parameter *Quality of Service* (Qos) untuk menilai *Throuhput*, *Delay*, *Jitter*, dan *Packet Loss*. Hasil dari penelitian ini adalah koneksi VPN yang stabil dan aman serta mendapatkan nilai *Quality of Service* yang baik.

Kata kunci: Jaringan, *Virtual Private Network*, *Layer 2 Tunneling Protocol*, IPSec, *Quality of Service*.

IMPLEMENTATION OF L2TP METHOD VPN NETWORK AS A SUPPORT NETWORK FOR FIELD WORKERS AT PT ALBANY CORONA LESTARI CIREBON BRANCH

Abstract

PT Albany Corona Lestari is a subsidiary of PT Indomarco PrismaTama which focuses on Indomaret store support in terms of electricity, network, hardware, and store employees. PT Albany Corona Lestari has workers in the office and field. In working, field workers rely on the Complaint Online website to check the list of incoming complaints, and ESS (*Employee Self Service*) for absences, input permits, and leave. Problems in accessing the Complain Online and ESS websites are an obstacle in working, because the website is only available in the local office network and the local Indomaret store network, so it cannot be accessed via the public network (internet). This problem can be overcome by using a VPN (*Virtual Private Network*) so that field worker devices such as laptops and smartphones can access the local office network and open the Complaint Online and ESS (*Employee Self Service*) websites from anywhere and anytime. The VPN used in this study is L2TP (*Layer 2 Tunneling Protocol*) with the addition of IPSec (*Internet Protocol Security*) as additional security. The installed L2TP VPN network is analyzed with *Quality of Service* (Qos) parameters to assess *Throuhput*, *Delay*, *Jitter*, and *Packet Loss*. The results of this study are a stable and secure VPN connection and get a good *Quality of Service* value.

Kata kunci: Network, *Virtual Private Network*, *Layer 2 Tunneling Protocol*, IPSec, *Quality of Service*.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

1. PENDAHULUAN

Pekerja lapangan merupakan pekerja yang bertugas untuk melakukan pekerjaan yang berada di luar kantor. Lokasi pekerja bisa saja masih berada di kota yang sama dengan kantor atau di luar kota tergantung kebutuhan perusahaan. Pekerja lapangan PT Albany Corona Lestari cabang Cirebon memiliki jangkauan area yang cukup luas, mulai dari Cirebon, Indramayu, Kuningan, Pemalang, Tegal, Brebes, Majalengka, Cilacap, Purwokerto, Banjar, Ciamis, Tasikmalaya, dan Pangandaran. Jumlah pekerja lapangan setiap daerah mengikuti luas daerah dan jumlah toko dalam suatu area agar pembagian pekerjaan setiap pekerja terbagi secara adil dan tidak memberatkan.

Dalam bekerja, pekerja lapangan berpatokan ke website complaint online yang isinya adalah daftar komplain dari toko yang harus mereka selesaikan dengan batas waktu setiap komplain selama tiga hari, jika lebih dari tiga hari maka akan mempengaruhi rating bulanan kantor cabang. Complaint online memiliki empat status komplain yaitu open yang artinya komplain belum dikerjakan oleh PIC (Personal In Charge) atau pekerja lapangan, inprogress yang artinya komplain sedang dalam proses pengerjaan oleh PIC, resolved yang artinya komplain selesai dikerjakan dan close yang artinya komplain sudah ditutup. Untuk pengajuan complaint online hanya bisa dilakukan melalui akun complaint online toko yang biasanya dilakukan oleh personel toko atau Area Supervisor dan untuk menutup komplain juga harus melalui akun toko. Sedangkan untuk mengubah status komplain dari open ke inprogress dan dari inprogress ke resolved dilakukan oleh PIC yang bertugas di area toko yang mengajukan komplain. Selain itu pekerja lapangan melakukan absen melalui website ESS (*Employee Self Service*) atau untuk mengisi cuti dan izin.

Saat ini website complaint online dan ESS masih berupa website lokal yang hanya dapat diakses dari jaringan kantor atau toko sehingga untuk mengecek komplain, absen, input izin dan cuti harus melalui jaringan toko atau meminta bantuan admin di kantor untuk membantu merekap komplain dan mengisi absen ESS pekerja lapangan. Hal ini menjadi penghambat dalam bekerja karena admin baru masuk kantor pukul delapan pagi dan komputer toko akan melakukan “initial” atau absen karyawan toko setiap paginya, sehingga pekerja lapangan paling cepat mendapat data

pekerjaan sekitar pukul setengah sembilan sampai setengah sepuluh.

Selain permasalahan website complaint online yang berada pada jaringan lokal, permasalahan koneksi jaringan toko juga dapat mengakibatkan perubahan status komplain dari open ke inprogress menjadi lebih lama karena toko tidak bisa mengakses website complaint online yang pada akhirnya harus diubah statusnya melalui admin di kantor. Waktu status komplain yang inprogress terlalu lama juga akan mempengaruhi rating bulanan kantor cabang, karena jika inprogress terlalu lama maka PIC dinilai terlalu lambat dalam bekerja. Ketergantungan pekerja lapangan dengan admin di kantor harus bisa diatasi karena admin tidak bisa 24 jam berada di kantor. Dan solusi yang paling tepat adalah membuat jaringan yang membuat pekerja lapangan dapat mengakses website lokal kantor dari manapun agar bisa terlepas dari ketergantungan meminta bantuan admin di kantor untuk mengakses website lokal kantor.

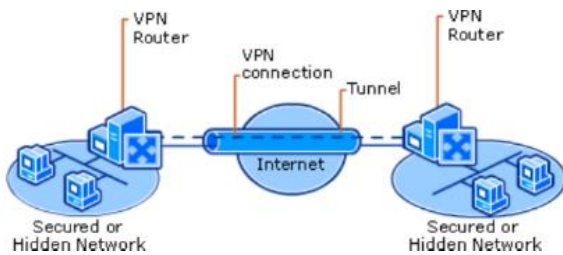
Salah satu solusi agar pekerja lapangan dapat mengakses website yang berada di jaringan lokal kantor adalah dengan menggunakan VPN (Virtual Private Network) untuk mengakses jaringan lokal kantor dari jaringan publik (internet). Penggunaan VPN untuk mengatasi masalah koneksi dari luar kantor ke dalam kantor merupakan solusi yang terbaik karena tidak harus menambah alat apapun dan konfigurasi yang tidak terlalu rumit. Dibandingkan dengan membuat website lokal kantor menjadi online yang konfigurasinya akan sangat rumit dan juga keamanan yang harus diperhatikan karena siapapun akan dapat mengakses jika website lokal menjadi online. Selain itu, dengan menggunakan VPN pegawai dapat mengirim file atau mengambil file melalui jaringan VPN ke jaringan lokal kantor.

2. BAHAN DAN METODE

Virtual Private Network (VPN) merupakan sebuah jaringan private yang menghubungkan satu jaringan ke jaringan lainnya dengan menggunakan jaringan internet. Data yang dilewatkan akan diencapsulation (dibungkus) dan dienkripsi agar data tersebut terjamin kerahasiaannya [1].

Virtual Private Network (VPN) adalah fasilitas yang menciptakan koneksi jarak jauh (remote access) menggunakan jaringan publik untuk akses Local Area Network (LAN) pada suatu jaringan. VPN merupakan cara untuk membuat sebuah

jaringan bersifat private dan aman dengan menggunakan jaringan publik seperti internet. VPN dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara point-to-point. Data dienkapsulasi dengan header yang berisi informasi routing (proses pengiriman data atau informasi dengan meneruskan paket data yang dikirim dari satu jaringan ke jaringan lainnya) untuk mendapatkan koneksi point-to-point sehingga dapat melewati jaringan publik dan dapat mencapai tujuan akhir.

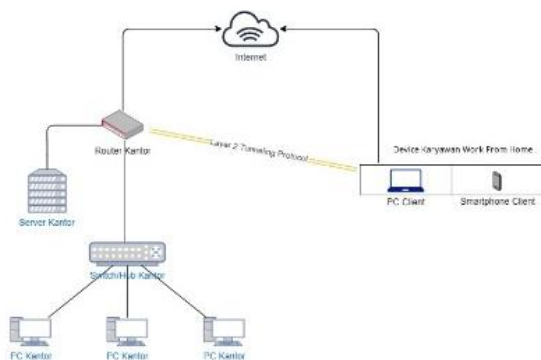


Gambar 2.1 Cara Kerja VPN

Sumber : [1]

3. HASIL DAN BAHASAN

Metode VPN yang digunakan adalah L2TP (*Layer 2 Tunneling Protocol*) yang merupakan protokol *tunneling* yang sering dipasang dengan protokol keamanan lain seperti IPSec untuk membuat koneksi VPN yang sangat aman. L2TP membuat terowongan antara dua titik koneksi L2TP, dan data dienkripsi oleh protokol IPSec dan menciptakan komunikasi yang aman antara terowongan (*tunnel*). L2TP juga merupakan pengembangan dari PPTP (*Point-to-Point Tunneling Protocol*) ditambah L2F (*Layer 2 Forwarding*), enkripsi yang digunakan sama dengan PPTP akan tetapi L2TP menggunakan UDP Port 1701 untuk melakukan komunikasi [2]. Pada Gambar 2.2 dapat dilihat gambaran implementasi L2TP.



Gambar 2.2 Gambaran VPN L2TP

Sebagai tambahan keamanan, jaringan VPN ini menggunakan IPSec (*Internet Protocol Security*) yang merupakan sekumpulan standar dan protokol yang bertujuan untuk menyediakan keamanan dan kerahasiaan

dalam pertukaran data di *layer network*. IPSec didefinisikan oleh sebuah badan internasional bernama IETF (*Internet Engineering Task Force*), yang terdiri dari para ilmuwan, praktisi, operator, dan vendor jaringan yang mempunyai misi untuk memajukan internet melalui penelitian dan pengembangan yang dilakukannya [1].

Dan untuk menguji kualitas jaringan peneliti menggunakan parameter *Quality of Service (QoS)* yang mengacu kepada kemampuan memberikan pelayanan berbeda kepada lalu lintas jaringan dengan kelas-kelas yang berbeda. Tujuan akhir dari QoS adalah memberikan network service yang lebih baik dan terencana dengan *dedicated bandwidth*, *jitter* dan *latency* yang terkontrol dan meningkatkan loss karakteristik. Berikut adalah penjelasan mengenai parameter-parameter yang digunakan dalam penilaian QoS yang baik [3] :

1. Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari source ke destination. Delay dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama [4]. Nilai delay TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*) dapat dilihat dalam Tabel 2.1.

Tabel 2.1 Indeks Delay TIPHON

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

Sumber : [4]

Persamaan untuk menghitung delay adalah :

$$Delay = \frac{Total\ Delay}{Total\ Paket\ yang\ diterima}$$

2. Jitter

Jitter atau variasi kedatangan yang diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan jitter. Jitter berhubungan erat dengan delay yang terjadi pada transmisi jaringan [4]. Pada Tabel 2.2 menunjukkan jitter menurut standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*).

Tabel 2.2 Indeks Jitter TIPHON

Kategori Degradasi	Peak 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

Sumber : [4]

Persamaan untuk menghitung jitter adalah :

$$Jitter = \frac{\text{Total Variasi Delay}}{\text{Total Paket yang diterima}}$$

Total variasi delay diperoleh dari :

$$\text{Delay} - \text{Rata - rata Delay}$$

3. Troughput

Troughput dapat diartikan sebagai kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second). *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada destination selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. *Throughput* merupakan kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan bandwidth karena *throughput* memang bisa disebut juga dengan bandwidth dalam kondisi yang sebenarnya. Bandwidth lebih bersifat fix sementara *throughput* sifatnya adalah dinamis tergantung trafik yang sedang terjadi [5]. Tabel 2.3 menunjukan *throughput* menurut standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*).

Tabel 2.3 Indeks Throughput TIPHON

Kategori Throughput	Throughput	Indeks
Sangat Bagus	76%-100%	4
Bagus	51%-75%	3
Sedang	26%-50%	2
Buruk	<25%	1

Sumber : [4]

Persamaan untuk menghitung *throughput* adalah :

$$\text{Throughput} = \frac{\text{Paket Data Diterima}}{\text{Lama Pengamatan}}$$

$$\text{Throughput} = \frac{\text{Throughput}}{\text{Bandwith Total}} \times 100$$

4. Packet Loss

Packet loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukan jumlah total paket yang hilang, dapat terjadi karena

collision dan congestion pada jaringan [4]. Tabel 2.4 menunjukan *throughput* menurut standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Network*).

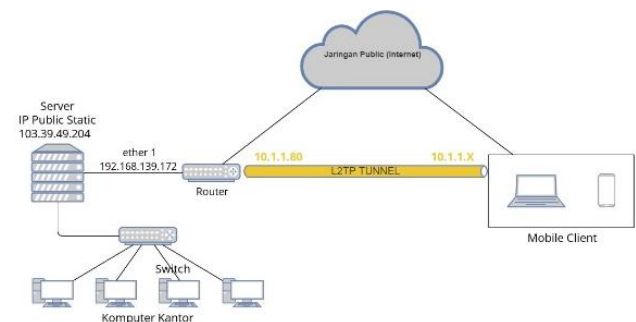
Tabel 2.4 Indeks Packet Loss TIPHON

Kategori Degredasi	Packet Loss	Indeks
Sangat Bagus	0%-2%	4
Bagus	3%-14%	3
Sedang	15%-24%	2
Buruk	>25%	1

Sumber : [4]

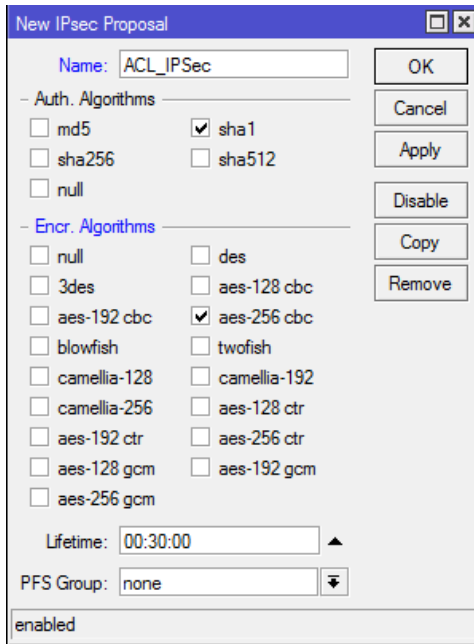
1. IMPLEMENTASI JARINGAN

Topologi pada implementasi jaringan VPN L2TP ini dapat dilihat pada Gambar 4.1.



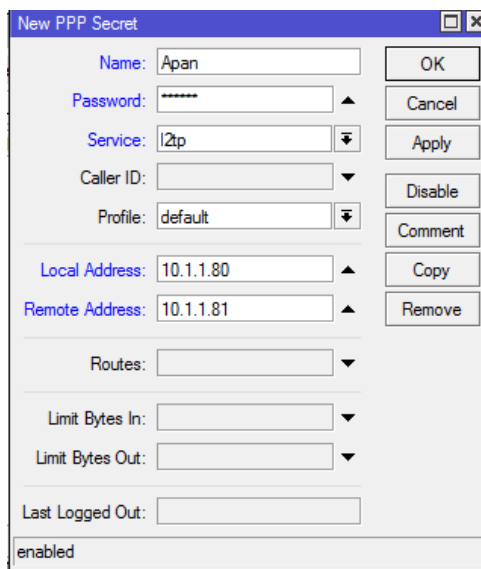
Gambar 4.1 Topologi Jaringan

Pada Topologi Gambar 4.1 dapat dilihat router tidak langsung terhubung ke modem, melainkan terhubung dengan server, karena dalam topologi peneliti menyesuaikan dengan jaringan yang sudah ada di kantor. Router harus memiliki akses ke internet atau jaringan publik agar dapat diakses melalui VPN. Setelah router tersambung dengan internet, setting IPSec seperti pad Gambar 4.2.



Gambar 4.2 Konfigurasi IPsec

Konfigurasi untuk akun *user client* atau PPP Secret seperti pada Gambar 4.2. Dalam PPP Secret terdapat *Local Address* yang berfungsi untuk menambahkan IP pada sisi VPN Server dalam jaringan VPN, dan *Remote Address* untuk IP pada sisi *client*.

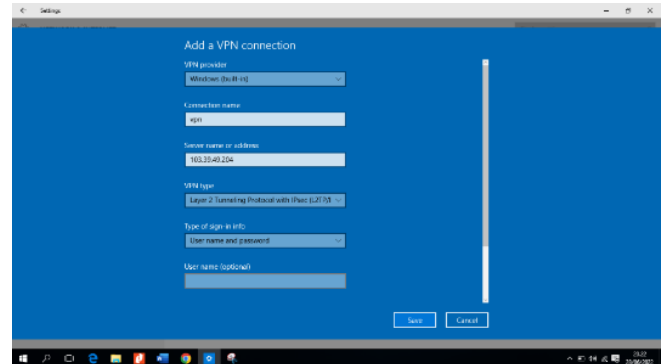


Gambar 4.3 PPP Secret

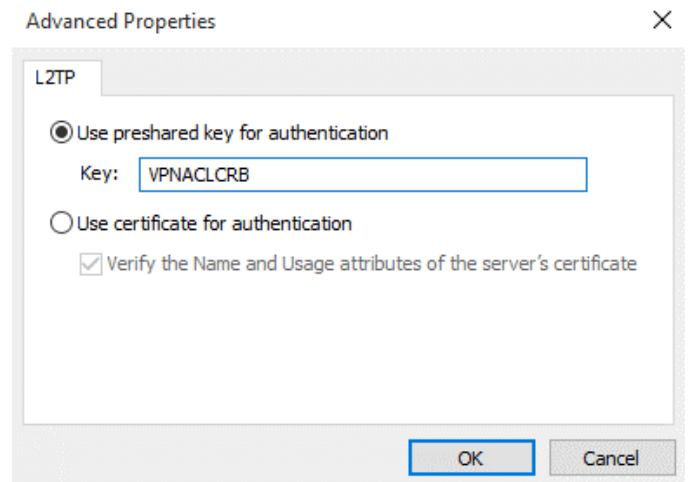
Kebutuhan perangkat keras untuk membangun sebuah infrastruktur jaringan VPN L2TP pada penelitian ini adalah:

1. Routerboard RB951UI-2HND.
2. Switch D-Link.
3. Kabel UTP Belden Cat6.
4. Modem atau internet kabel Icon+.
5. Konektor RJ45 AMP Cat6.

Konfigurasi di sisi *client* cukup memasukkan IP *address* publik milik server, *username*, *password*, dan *key* IPsec. Contohnya seperti pada Gambar 4.4 dan 4.5 dengan menggunakan laptop sebagai *client*.



Gambar 4.4 Konfigurasi Client VPN



Gambar 4.5 Input Key IPsec

2. PENGUJIAN JARINGAN

Pengujian ini bertujuan memastikan jaringan VPN L2TP berjalan dengan baik dan sudah dapat digunakan untuk penunjang pekerja lapangan. Pada pengujian ini, penulis menggunakan Laptop ACER X540L dengan koneksi internet dari *provider* "by.U" untuk melakukan *remote access* melalui VPN L2TP ke jaringan lokal kantor agar dapat mengakses website lokal kantor.

Pengujian pertama dengan melakukan ping ke IP VPN L2TP pada router server untuk memastikan bahwa koneksi melalui jaringan VPN, ditujukan pada Gambar 5.1.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Apriyadi>ping 10.1.1.80

Pinging 10.1.1.80 with 32 bytes of data:
Reply from 10.1.1.80: bytes=32 time=52ms TTL=64
Reply from 10.1.1.80: bytes=32 time=68ms TTL=64
Reply from 10.1.1.80: bytes=32 time=57ms TTL=64
Reply from 10.1.1.80: bytes=32 time=44ms TTL=64

Ping statistics for 10.1.1.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 44ms, Maximum = 68ms, Average = 55ms

C:\Users\Apriyadi>

```

Gambar 5.1 Tes Koneksi IP VPN Server

Kemudian pengujian ping dengan salah satu IP Adreess dari jaringan lokal kantor untuk menguji koneksi jaringan VPN dengan jaringan lokal kantor. Ditunjukkan pada Gambar 5.2.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Apriyadi>ping 192.168.39.83

Pinging 192.168.39.83 with 32 bytes of data:
Reply from 192.168.39.83: bytes=32 time=61ms TTL=64
Reply from 192.168.39.83: bytes=32 time=61ms TTL=64
Reply from 192.168.39.83: bytes=32 time=58ms TTL=64
Reply from 192.168.39.83: bytes=32 time=42ms TTL=64

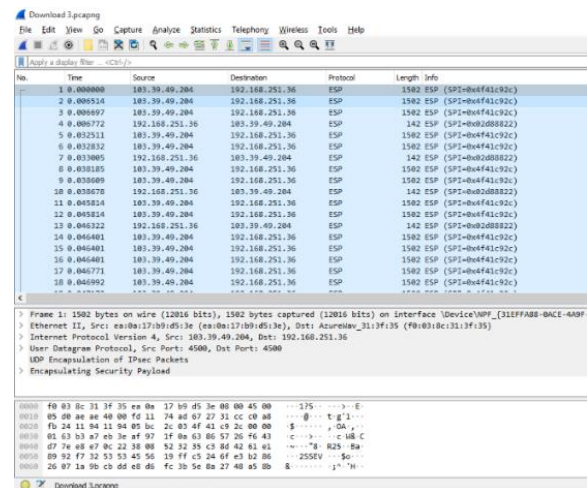
Ping statistics for 192.168.39.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 42ms, Maximum = 61ms, Average = 55ms

C:\Users\Apriyadi>

```

Gambar 5.2 Tes Koneksi IP VPN Server

Selanjutnya pengujian keamanan menggunakan aplikasi Wireshark. Hasil dari pengujian ini menunjukkan paket data yang melewati jaringan VPN dienkripsi oleh IPSec dengan protokol ESP. Hasilnya dapat dilihat pada Gambar 5.3.



Gambar 5.3 Tes Koneksi IP VPN Server

Pengujian selanjutnya menggunakan paramete *Quality of Service (QoS)* untuk menguji kualitas dari jaringan VPN L2TP. Pengujian dilakukan dengan cara *upload* dan *download* file sebesar 7mb melalui FTP (*File Transfer Protocol*).

1. Delay

Hasil dari pengujian *delay* dari *download* file adalah :

$$Delay = \frac{Total\ Delay}{Total\ Paket\ yang\ diterima}$$

$$Delay = \frac{17,5931}{7779} = 0,002262s$$

$$Delay = 0,002262s \times 1000 = 2,26ms$$

Dan hasil dari pengujian *delay* dari *upload* file adalah :

$$Delay = \frac{Total\ Delay}{Total\ Paket\ yang\ diterima}$$

$$Delay = \frac{20,5706}{8466} = 0,002814s$$

$$Delay = 0,002814s \times 1000 = 2,81ms$$

2. Jitter

Hasil dari pengujian *jitter* dari *download* file adalah :

$$Jitter = \frac{Total\ Variasi\ Delay}{Total\ Paket\ yang\ diterima - 1}$$

$$Jitter = \frac{17,6884}{7778}$$

$$Jitter = 0,002274s$$

$$Jitter = 2,27ms$$

Dan hasil dari pengujian *jitter* dari *upload* file adalah :

$$Jitter = \frac{Total\ Variasi\ Delay}{Total\ Paket\ yang\ diterima - 1}$$

$$Jitter = \frac{20,57046}{8465}$$

$$Jitter = 0,00243s$$

$$Jitter = 2,43ms$$

3. Troughput

Hasil dari pengujian *troughput* dari *download* file adalah :

$$Throughput = \frac{Paket\ Data\ Diterima}{Lama\ Pengamatan}$$

$$Throughput = \frac{7999716}{17,593} = 454.710,2\ Bps$$

$$Throughput = 454.710,2 \times \frac{8}{1000} kbps$$

$$Throughput = 3637\ kbps$$

$$Throughput = \frac{Throughput}{Bandwith\ Total} \times 100$$

$$Throughput = \frac{3637}{4096} \times 100$$

$$Throughput = 88,8\ %$$

Dan hasil dari pengujian *troughput* dari *upload* file adalah :

$$Throughput = \frac{Paket\ Data\ Diterima}{Lama\ Pengamatan}$$

$$Throughput = \frac{8705380}{20,571} = 423.187\ Bps$$

$$Throughput = 423.187 \times \frac{8}{1000} kbps$$

$$Throughput = 3385\ kbps$$

$$Throughput = \frac{Throughput}{Bandwith\ Total} \times 100$$

$$Throughput = \frac{3385}{4096} \times 100$$

$$Throughput = 82,6\ %$$

4. Packet Loss

Hasil dari pengujian *packet loss* dari *download* file adalah :

$$Packet\ Loss = \frac{Paket\ dikirim - Paket\ diterima}{Paket\ dikirim} \times 100\%$$

$$Packet\ Loss = \frac{7779 - 7779}{7779} \times 100\%$$

$$Packet\ Loss = 0\ %$$

Dan hasil dari pengujian *packet loss* dari *upload* file adalah :

$$Packet\ Loss = \frac{Paket\ dikirim - Paket\ diterima}{Paket\ dikirim} \times 100\%$$

$$Packet\ Loss = \frac{8466 - 8466}{8466} \times 100\%$$

$$Packet\ Loss = 0\ %$$

5. Analisa Quality of Service

Hasil *Quality of Service* Jaringan VPN L2TP berdasarkan data yang diambil menggunakan Wireshark dan menghitung *Throughput*, *Delay*, *Jitter*, dan *Packet Loss* dari *Download* dan *Upload* Video dapat dilihat pada Tabel 5.1.

Tabel 5.1 Tabel Quality of Service VPN L2TP

Pengukuran	Parameter QoS	Hasil	Indeks	Kualitas (TIPHON)
Download	Throughput	88,8%	4	Sangat Bagus
	Delay	2,26ms	4	Sangat Bagus
	Jitter	2,27ms	3	Bagus
	Packet Loss	0%	4	Sangat Bagus
Upload	Throughput	82,6%	4	Sangat Bagus
	Delay	2,43ms	4	Sangat Bagus
	Jitter	2,43ms	3	Bagus
	Packet Loss	0%	4	Sangat Bagus

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan yang dimulai dari penentuan pokok permasalahan, analisis sistem sampai pengimplementasian jaringan VPN (*Virtual Private Network*) L2TP (*Layer 2 Tunneling Protocol*) pada kantor PT Albany Corona Lestari Cabang Cirebon, penulis mendapatkan kesimpulan dan saran sebagai berikut:

1. Koneksi jaringan dari *Mobile Client* atau pekerja lapangan berjalan dengan baik tanpa adanya hambatan dalam akses dari jaringan publik ke jaringan lokal kantor sehingga pekerja lapangan dapat mengakses jaringan lokal kantor untuk membuka *website* ESS (*Employee Self Service*) untuk melakukan absensi, input izin, dan cuti, dan juga dapat mengakses *website* *Complaint Online* dari mana saja dan kapan saja untuk memeriksa daftar komplain yang diterima dari toko Indomaret, selama perangkat *client* memiliki akses *internet*.
2. IPsec (*Internet Protocol Security*) pada jaringan VPN (*Virtual Private Network*) L2TP (*Layer 2 Tunneling Protocol*) terbukti dapat mengenkripsi paket data yang melewati jaringan VPN dengan protokol ESP (*Encapsulating Security Payload*) agar paket data tidak dapat dilihat oleh peretas, sehingga dapat disimpulkan bahwa jaringan VPN L2TP ini aman untuk diakses dari jaringan publik.
3. Parameter *Quality of Service* dapat menjadi acuan dalam menilai kualitas jaringan agar jika hasil

pengujian Quality of Service kurang baik, dapat diperbaiki instalasi jaringannya. Quality of Service jaringan VPN L2TP pada penelitian ini mendapatkan nilai Sangat Bagus dengan indeks nilai 4 pada pengujian Throughput, Delay, dan Packet Loss dari Download dan Upload video, dan mendapat nilai Bagus dengan indeks nilai 3 pada Jitter dari Download dan Upload video.

4. Penelitian selanjutnya dapat menambahkan DHCP (*Dynamic Host Configuration Protocol*) untuk PPP Secret agar pemberian IP Remote dapat terisi otomatis dan satu akun client dapat digunakan lebih dari satu perangkat secara bersamaan.
5. Menggunakan protokol keamanan berbeda selain IPSec atau menggunakan *Authentication Algorithm* dan *Encryption Algorithm* selain yang digunakan pada penelitian ini.

Menggunakan IP address publik yang dynamic untuk koneksi internet VPN Server agar jika terjadi permasalahan pada jaringan internet pada Provider yang menyediakan IP address publik yang static VPN dapat terus aktif.

5. DAFTAR PUSTAKA

- [1]F. Sjafrina, “Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional,” *Proc. Semin. Nas. Teknol. Inf. dan Komun. STI&K (SeNTIK 2019)*, vol. 3, pp. 211–217, 2019.
- [2]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, Mar. 2020, doi: 10.35940/ijrte.f8335.038620.
- [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]I. K. S. Satwika, “Analisis Quality of Service Jaringan Virtual Private Network (Vpn) Di Stmik Stikom Indonesia,” *J. Ilm. Inform.*, vol. 7, no. 01, p. 60, 2019, doi: 10.33884/jif.v7i01.1016.