

# IMPLEMENTATION OF VPN USING THE PPTP METHOD TO ACCESS CCTV MONITORING DATA AT THE BUKIT RAYA DISTRICT OFFICE

## PENERAPAN VPN MENGGUNAKAN METODE PPTP UNTUK MENGAKSES DATA MONITORING CCTV DI KANTOR KECAMATAN BUKIT RAYA

Linna Oktaviana Sari<sup>1</sup>, Tiara Dwi Kharisma<sup>2</sup>

Teknik Informatika, Universitas Riau

Kampus Binawidya Jl. HR Soebrantas KM 12.5, Simpang Baru, Pekanbaru

Email: linnaosari@lecturer.unri.ac.id<sup>1</sup>, tiara.dwi5610@student.unri.ac.id<sup>2</sup>

**Abstract** - Bukit Raya District faces challenges in monitoring activities across five scattered sub-districts, as well as employees frequently being absent from the office during working hours. To address this issue, the installation of a CCTV system is crucial for monitoring employee performance and office activities. However, remote access to CCTV data is not yet available. This study aims to implement a VPN using the PPTP (Point to Point Tunneling Protocol) method to allow CCTV monitoring data in sub-district offices to be securely and stably accessed from the district office. PPTP was chosen due to its cross-platform support and ease of configuration and maintenance. The implementation was carried out in two sub-districts, Tangkerang Selatan and Simpang Tiga. The results indicate that the PPTP VPN successfully connected the district office to these sub-districts, enabling secure remote access to CCTV data. Quality of Service (QoS) testing demonstrated network performance improvements in terms of throughput, packet loss, delay, and jitter. Therefore, this system effectively enhances operational efficiency and security in Bukit Raya District.

**Keywords** – VPN, PPTP CCTV, Quality of Service (QoS)

**Abstrak** – Kantor Kecamatan Bukit Raya menghadapi tantangan dalam memantau aktivitas di lima kelurahan yang tersebar, serta pegawai yang sering tidak berada di kantor selama jam kerja. Untuk mengatasi hal ini, pemasangan sistem CCTV menjadi penting guna memantau kinerja pegawai dan aktivitas di kantor. Namun, akses jarak jauh terhadap data CCTV belum tersedia. Penelitian ini bertujuan untuk menerapkan VPN menggunakan metode PPTP (Point to Point Tunneling Protocol) agar data monitoring CCTV di kantor kelurahan dapat diakses dari kantor kecamatan secara aman dan stabil. PPTP dipilih karena mendukung berbagai platform dan mudah dalam konfigurasi serta pemeliharaan. Implementasi dilakukan pada dua kelurahan, yaitu Kelurahan Tangkerang Selatan dan Kelurahan Simpang Tiga. Hasil penelitian menunjukkan bahwa VPN PPTP berhasil menghubungkan kantor kecamatan dengan dua kelurahan tersebut, memungkinkan akses jarak jauh yang aman terhadap data CCTV. Pengujian Quality of Service (QoS) memperlihatkan peningkatan performa jaringan dari segi throughput, packet loss, delay, dan jitter. Dengan demikian, sistem ini efektif dalam meningkatkan efisiensi operasional dan keamanan di Kecamatan Bukit Raya.

**Kata Kunci** - VPN, PPTP CCTV, Quality of Service

## I. PENDAHULUAN

Dalam era globalisasi dan kemajuan teknologi informasi, penggunaan sistem pemantauan CCTV telah menjadi sangat penting untuk pengawasan di berbagai lingkungan seperti sekolah, perusahaan, dan pusat perbelanjaan. Namun, untuk memonitor CCTV dengan efektif, diperlukan jaringan yang stabil, dan cepat. Salah satu solusi untuk ini adalah penggunaan VPN (*Virtual Private Network*), yang memungkinkan komunikasi jaringan yang lebih privat melalui sistem tunneling. VPN dapat menghubungkan jaringan di berbagai lokasi secara aman, misalnya antara kantor kecamatan dan kelurahan. Di Kecamatan Bukit Raya, terdapat permasalahan seperti sulitnya mengawasi aktivitas di lima kelurahan yang tersebar, serta pegawai yang sering tidak berada di kantor saat jam kerja. Untuk itu, pemasangan sistem CCTV sangat diperlukan untuk memantau kinerja pegawai dan kegiatan di kantor tersebut. Namun, saat ini CCTV di kelurahan belum dapat diakses secara jarak jauh dari kantor kecamatan.

Penelitian ini bertujuan untuk menerapkan VPN menggunakan metode PPTP (*Point to Point Tunneling Protocol*) untuk memonitor CCTV dari kantor kecamatan ke kantor kelurahan. PPTP dipilih karena mendukung berbagai platform dan mudah dalam konfigurasi serta pemeliharannya. Implementasi ini dimulai dengan kantor Kelurahan Tangkerang Selatan dan Kelurahan Simpang Tiga, dan jika berhasil, akan diperluas ke kelurahan lainnya. Terdapat jurnal penelitian terdahulu sebagai referensi utama pada penelitian ini yang akan di gunakan dimana [1] penelitian ini berhasil menerapkan metode *Point to Point Tunelling Protokol* (PPTP) pada VPN, jaringan komputer yang digunakan dalam mengatasi permasalahan yang terjadi antar kantor yang jaraknya berjauhan, ini dapat memudahkan pekerjaan pada pihak pekerja IT dan juga memberi keamanan dalam pengiriman data yang di transmisikan, di *enkripsi*-kan dalam jaringan *private*, sehingga pekerjaan yang di buat terjaga keamanan dari pihak yang tidak bertanggung jawab [2].

Pada penelitian ini memilih PPTP sebagai metode yang digunakan karna memiliki kinerja yang lebih baik di banding protocol lainnya kare menggunakan nekripsi yang lebih sederhana yang dapat mengurangi beban pada perangkat keras, sehingga kinerja hasil koneksinya lebih stabil dan cepat. [3] PPTP juga di dukung hampir semua sistem operasi utama tanpa perlu konfigurasi yang rumit. Di banding protocol yang lain seperti L2TP atau IPSec, PPTP ini dapat membantu pada kassus penelitian ini yang dimana fokus pada kecepatan dan kompatibilitas dari pada keamanan yang sangat ketat. Kebutuhan monitoring ini sudah cukup untuk bisa mengatasinya. [4]. Dengan penerapan VPN ini, diharapkan data monitoring CCTV dapat diakses hanya oleh divisi IT dan kepala kantor kecamatan, memastikan privasi dan keamanan data. Metode PPTP menyediakan saluran terenkripsi yang efektif untuk mengakses data monitoring CCTV secara stabil dan cepat, sehingga mempermudah pengawasan dan meningkatkan efisiensi operasional di Kecamatan Bukit Raya.

## II. SIGNIFIKANSI STUDI

### A. Penelitian Terdahulu

Dalam referensi karya ilmiah [1] berhasil menerapkan metode *Point to Point Tunneling Protokol* (PPTP) pada VPN, jaringan komputer yang digunakan dalam mengatasi permasalahan yang terjadi antar kantor yang jaraknya berjauhan, ini dapat memudahkan pekerjaan pada pihak pekerja IT dan juga memberi keamanan dalam pengiriman data yang di transmisikan, di *enkripsi*-kan dalam jaringan *private*, sehingga pekerjaan yang di buat terjaga keamanan dari pihak yang tidak bertanggung jawab.

Penelitian yang di buat [5] ini berhasil menerapkan VPN dengan Metode *Point to Point Tunneling Protokol* (PPTP), untuk menghubungkan Gedung A dengan Gedung B dengan baik dan juga proses dalam pengiriman data dilakukan dengan sukses dan lancar. VPN dengan menggunakan metode protokol PPTP ini, dapat digunakan untuk menghubungkan jaringan dengan aman walaupun menggunakan jaringan public sekalipun. Jurnal penelitian [6] penelitian ini dapat melakukan pengujian dalam menghubungkan jaringan yang di kantor pusat dapat terhubung ke kantor cabang dengan menerapkan VPN menggunakan metode *Point to Point Tunneling Protokol* (PPTP) dan pada pertukaran data antar kantor mereka menggunakan aplikasi hamachi yang dimana aplikasi ini merupakan aplikasi VPN (*Virtual Private Network*).

### B. Landasan Teori

Jaringan komputer merupakan implementasi dari komunikasi data yang dimana data yang di kirim pasti di terima komputer yang di tuju dengan waktu yang cepat[7]. Dimana jaringan memiliki kriteria tertentu yang wajib dipenuhi supaya tercapainya dari dasar komunikasi data. Kriteria yang penting dimiliki jaringan komputer ada 3, *reliability, performance dan Security*. [8]. Virtual Private Network (VPN) adalah teknologi yang digunakan untuk mengenkripsi dan mengamankan koneksi melalui jaringan publik, seperti internet atau WiFi hotspot. VPN meningkatkan privasi dengan mengganti IP awal pengguna dengan IP lain yang disediakan oleh penyedia VPN.[9] VPN memungkinkan pengguna untuk terhubung ke jaringan pribadi secara virtual, seolah-olah mereka berada dalam satu jaringan yang sama meskipun berada di lokasi berbeda. [10] PPTP (*Point to Point Tunneling Protokol*) merupakan sebuah protokol atau metode komunikasi yang memungkinkan terjadinya komunikasi antara titik terhadap jaringan internet dengan membuat VPN [4]. Metode atau protokol VPN, yang digunakan untuk mengatur koneksi dan memfasilitasi komunikasi aman melalui internet dan juga dapat mengamankan transfer data melalui jaringan public, seperti Internet. PPTP yang di kembangkan oleh perusahaan skala besar yang dapat mengkoneksikan jaringan satu ke jaringan lain menggunakan jalur private menggunakan internet. [11]. QoS Pada penelitian ini akan menggunakan pengujian QoS yang akan mengukur kecepatan jaringan sebelum dan sesudah penerapan VPN PPTP. QoS memiliki beberapa pengukuran parameter yaitu *throughput, packet loss, delay dan jitter*. [12] Masing masing pengukuran memiliki rumus masing masing, diantaranya:

1. *Throughput* merupakan jalur komunikasi yang memiliki kapasitas maksimum untuk mentransfer data dalam bentuk satuan waktu tertentu, dimana satuan ukurannya *bit per second* (bps)[13]. Untuk menghitung *throughput* dapat menggunakan rumus persamaan 2.1 berikut:

$$\textit{Throughput} = \frac{\textit{Total Data Transferred}}{\textit{Total Time}} \quad (1)$$

Untuk melihat kategori *throughput* berdasarkan indeksnya dapat di lihat tabel indeks parameter *throughput* 2.2.

TABEL I  
INDEKS PARAMETER THROUGHPUT

<b>Indeks Parameter <i>Throughput</i></b>		
<b>Kategori <i>Throughput</i></b>	<b><i>Throughput</i> (%)</b>	<b>Indeks</b>
Sangat Bagus	76 -100 %	4
Bagus	51 -75 %	3
Sedang	26 – 50 %	2
Buruk	< 25 %	1

2. *Packet Loss*

*Packet Loss* merupakan persentase paket data yang hilang atau gagal sampai ketujuan yang biasanya terjadi karena kemacetan jaringan atau keerusakan data. [14]. Untuk menghitung *packet loss* dapat menggunakan rumus persamaan 2.2 berikut:

$$\textit{Packet Loss} = \frac{(\textit{Paket dikirim-paket di terima})}{\textit{Paket dikirim}} \times 100\% \quad (2)$$

Untuk melihat kategori *packet loss* berdasarkan indeksnya dapat di lihat tabel indeks parameter *packet loss* 2.3.

TABEL II  
INDEKS PARAMETER PACKET LOSS

<b>Indeks Parameteer <i>Packet Loss</i></b>		
<b>Kategori <i>Packet Loss</i></b>	<b><i>Packet Loss</i> (%)</b>	<b>Indeks</b>
Buruk	< 25 %	1
Sedang	12% - 24%	2
Bagus	3% - 11%	3
Sangat Bagus	0-2%	4

3. *Delay*

*Delay* merupakan waktu yang dibutuhkan oleh data untuk berpindah dari satu titik ke titik lainnya dalam jaringan.[15] Untuk menghitung *delay* dapat menggunakan rumus persamaan 2.3 berikut:

$$\textit{Delay} = \frac{\textit{Total Delay}}{\textit{Total paket yang diterima}} \quad (3)$$

Untuk melihat kategori *delay* berdasarkan indeksnya dapat di lihat tabel indeks parameter *delay* 2.4.

TABEL III  
INDEKS PARAMETER DELAY

<b>Indeks Parameteer Delay</b>		
<b>Kategori Delay</b>	<b>Delay (ms)</b>	<b>Indeks</b>
Sangat Bagus	<150ms	4
Bagus	150ms - 300ms	3
Sedang	300ms - 400ms	2
Buruk	>450	1

#### 4. Jitter

*Jitter* merupakan variasi *delay* dalam pengiriman paket data, biasanya penyebab karena ketidak stabilan dalam *streaming* atau panggilan suara. Untuk menghitung *jitter* dapat menggunakan rumus persamaan 2.4 berikut:

$$Jitter = \frac{Total\ Variasi\ Jitter}{Total\ paket\ yang\ diterima - 1} \quad (4)$$

Untuk melihat kategori *Jitter* berdasarkan indeknya dapat di lihat tabel indeks parameter *Jitter* 2.5. [16]

TABEL IV  
INDEKS PARAMETER JITTER

<b>Indeks Parameteer Jitter</b>		
<b>Kategori Jitter</b>	<b>Jitter (ms)</b>	<b>Indeks</b>
Sangat Bagus	0ms	4
Bagus	0ms – 74 ms	3
Sedang	75ms – 124ms	2
Buruk	125ms - 225ms	1

### C. Lokasi penelitian



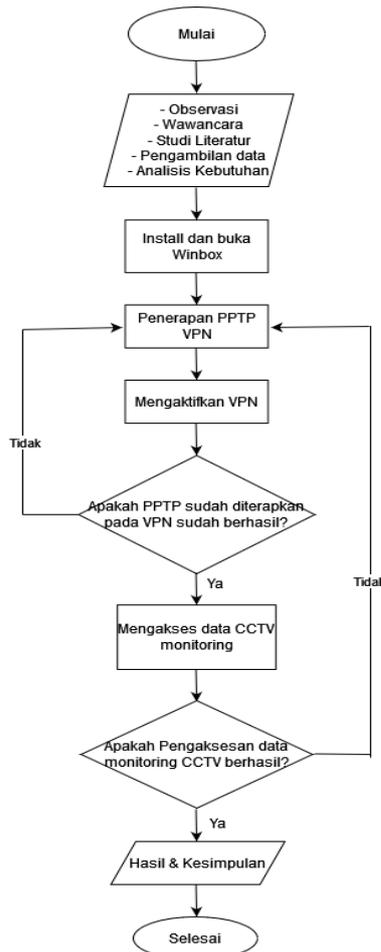
Gambar 1. Kantor Camat Bukit Raya

Kecamatan Bukit Raya merupakan sebuah kecamatan yang ada di kota Pekanbaru, yang dimana salah satu instansi yang bergerak di bidang pelayanan masyarakat. Lokasi dan Wilayah Administratif Kantor Kecamatan Bukitraya beralamat di Jalan Kaharuddin Nasution No. 37, Pekanbaru. Kecamatan bukit raya memiliki 5 kelurahan di antaranya:

1. Kelurahan Dimpang Tiga, 2
2. Kelurahan Tangkerang Labuai
3. Kelurahan Tangkerang Selatan
4. Kelurahan Tangkerang Utara
5. Kelurahan Air Dingin

### D. Metode penelitian

Penelitian ini menjelaskan tentang bagaimana tahapan penelitian dalam penerapan VPN untuk mengambil data CCTV monitoring menggunakan metode PPTP dari awal sampai akhir penelitian. Tahapan metodologi yang akan di lakukan di tujukan pada Gambar 2 sebagai berikut

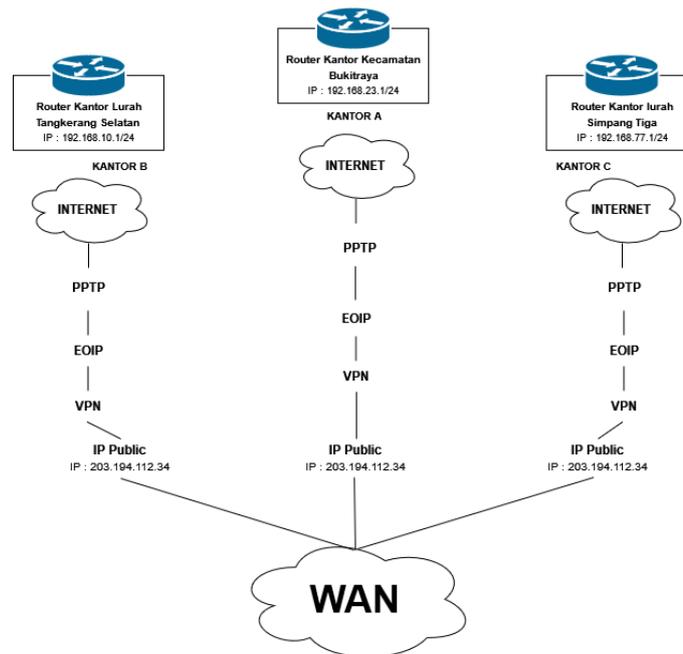


Gambar 2. Tahapan Metodologi Penelitian

Pada gambar 2 merupakan tahapan tahapan yang akan di lakukan pada peneltian ini di mulai dari identifikasi sampai hasil dan kesimpulan.

#### Ilustrasi cara kerja VPN PPTP

Pada tahapan penerapan VPN ini di lakukan pada kantor A (Kecamatan Bukitraya) sebagai server yang akan mengambil data monitoring CCTV dari 2 kantor B (Kelurahan Tangkerang Selatan) dan kantor C (Kelurahan Simpang Tiga). Dapat di lihat pada gambar 3 ilustrasi bagaimana VPN PPTP di terapkan.



Gambar 3. Cara Kerja VPN PPTP

Pada gambar 3 VPN PPTP ini menghubungkan kantor kecamatan dan kelurahan menggunakan mikrotik yang masing-masing memiliki IP berbeda: mikrotik A (192.168.23.1/24), mikrotik B (192.168.10.1/24), dan mikrotik C (192.168.77.1/24). Setiap mikrotik terhubung ke internet melalui Wi-Fi dengan IP publik dari server. Untuk menghubungkan jaringan secara jarak jauh, digunakan EOIP sebagai tunneling antar router mikrotik melalui IP tadi. Setelah tunnel terbentuk, WAN digunakan untuk menghubungkan kantor dan penyimpanan cloud secara bersamaan.

Cara kerja VPN PPTP ini di lakukan pada kantor A (Kecamatan Bukitraya) sebagai server yang akan mengambil data monitoring CCTV dari 2 *client* yaitu kantor B (Kelurahan Tangkerang Selatan) dan kantor C (Kelurahan Simpang Tiga). Berikut

Algoritma cara kerjanya.



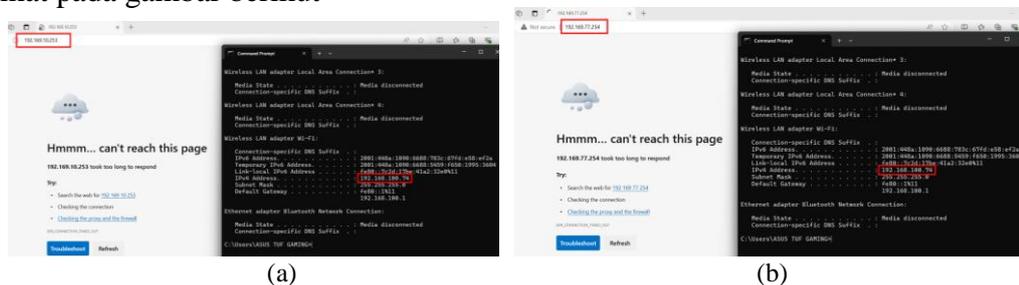
Gambar 4. Blok Diagram Cara Kerja PPTP

Pada Gambar 4 menjelaskan algoritma cara kerja PPTP yang dimana PPTP ini akan membungkus lagi paket PPP. Berikut penjelasan dari Algoritma cara kerja PPTP:

1. **Memulai Koneksi:** Kantor B dan C meminta koneksi ke Kantor A melalui TCP pada port 1723, lalu Kantor A merespons dan membuat koneksi kontrol.
2. **Membangun Terowongan GRE:** Kantor B dan C mengirimkan permintaan koneksi PPTP, dan Kantor A merespons. Mereka bertukar pesan untuk memastikan koneksi aktif.[17]
3. **Otentikasi dan Konfigurasi PPP:** Kantor B dan C memulai negosiasi protokol PPP, Kantor A merespons, dan otentikasi dilakukan menggunakan PAP, CHAP, atau MS-CHAP.
4. **Mengirim Data:** Data dikirim melalui terowongan dengan paket dienkapsulasi dalam frame PPP dan GRE. Data asli diambil di sisi penerima.
5. **Putus Koneksi:** Kantor A atau Kantor B/C mengirimkan permintaan untuk menghentikan koneksi, dan terowongan ditutup.

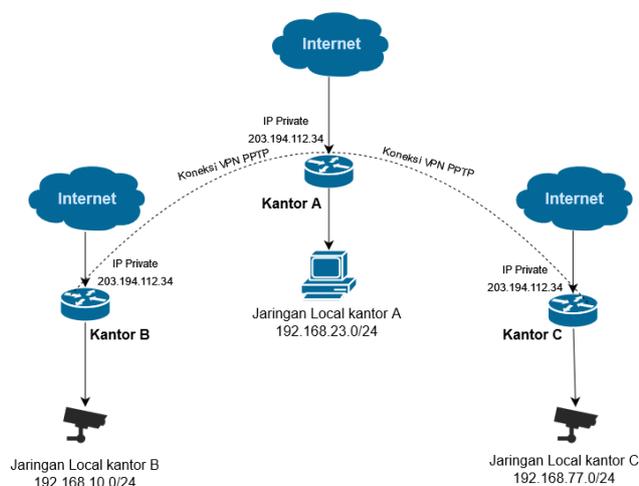
### III. HASIL DAN PEMBAHASAN

Untuk membuktikan hasil koneksi VPN sudah di terapkan, lakukan pengujian dengan memasukkan IP Address luar yang mencoba masuk untuk mengakses data CCTV monitoring. Dapat dilihat pada gambar berikut



Gambar 6. (a) IP Address Luar Mengakses CCTV Kantor B, (b) IP Address Luar Mengakses CCTV Kantor C

Pada gambar diatas merupakan hasil koneksi VPN yang dimana IP Address luar (192.168.100.74) tidak berhasil mengakses data CCTV monitoring pada kantor B dan C.



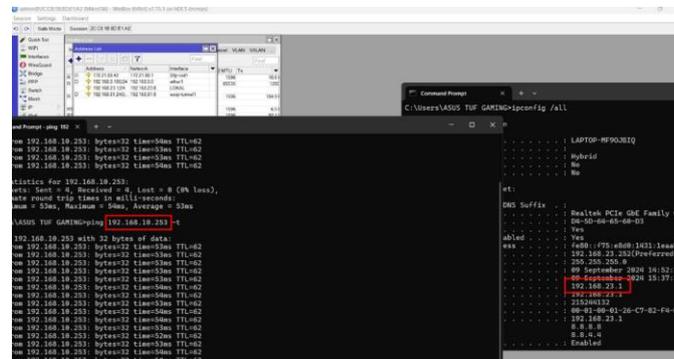
Gambar 5. Topologi VPN PPTP yang sudah di terapkan

Pada Gambar di atas merupakan hasil ilustrasi kerja VPN PPTP, pada masing masing kantor memiliki IP Publik yang berbeda, dengan VPN PPTP ke 3 router dapat saling terkoneksi dengan

menggunakan IP *private*, sehingga tidak dapat di akses langsung oleh orang lain melalui Internet.

Berikut merupakan hasil konfigurasi VPN PPTP antar 3 router mikrotik yang dimana koneksi antar 3 kantor yaitu kantor A (Kecamatan Bukitraya) sudah terkoneksi dengan 2 kantor yaitu kantor B (kantor Kelurahan Tangkerag Selatan) dan kantor C (kantor Kelurahan Simpang Tiga). Untuk pembuktian antar 3 router yang saling terkoneksi

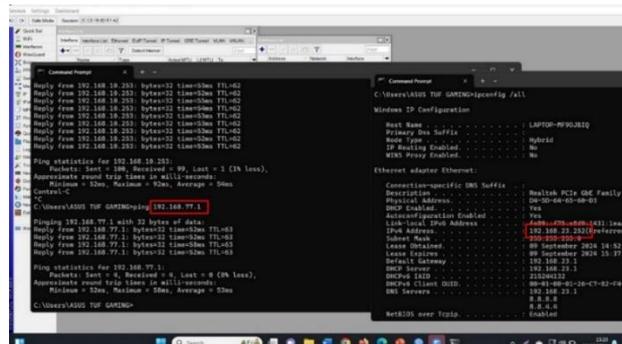
Router kantor A dan kantor B



Gambar 6. Router Kantor A Ping Ke Router Kantor B

Pada gambar diatas dimana IP *address* router A (192.168.23.1) dan router B (192.168.10.1) melakukan ping yang dimana dapat di lihat pada gambar 8 yaitu router kantor A berhasil ping router yang di kantor B, dapat dilihat bahwa *reply* berjalan.

Router kantor A dan kantor C

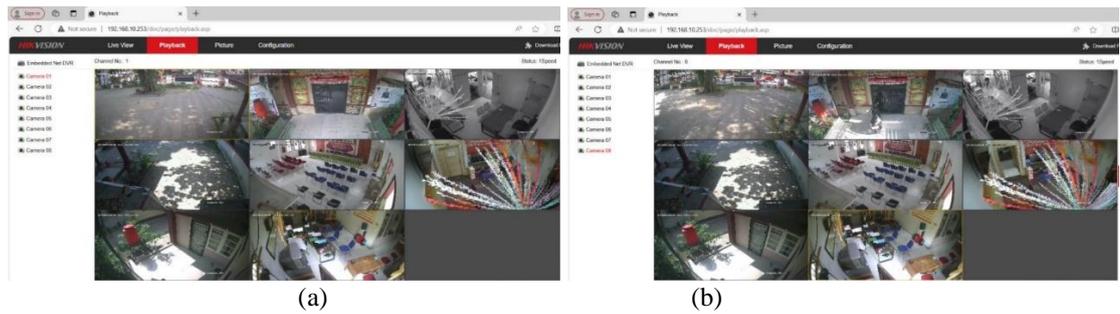


Gambar 7. Router Kantor A Ping ke router kantor C

Pada gambar 7 diatas dimana IP *address* router A (192.168.23.1) dan router C (192.168.77.1) melakukan ping yang dimana dapat di lihat pada gambar 9 yaitu router kantor A juga berhasil ping router yang di kantor B, dapat dilihat bahwa *reply* berjalan.

Dari hasil pengujian monitoring data CCTV yang telah bisa di akses secara jarak jauh. Dimana kantor A (Kecamatan Bukitraya) dapat memantau CCTV kantor B (Kelurahan Tangkerag Selatan) dan Kantor C (Kelurahan Simpang Tiga).

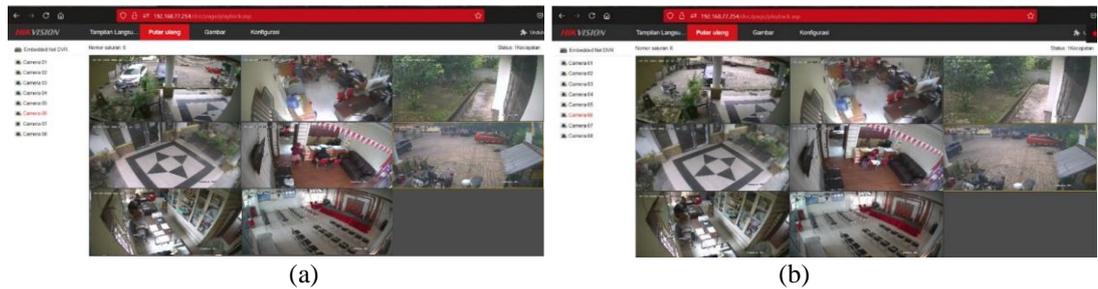
Kantor A mengakses CCTV kantor B



Gambar 8. (a), (b) Prview kantor Kelurahan Tangerang Selatan

Pada gambar 8 merupakan priview CCTV kantor B yang dapat di akses jarak jauh oleh kantor A. priview gambar 8 di ambil pada gambar di pagi hari, gambar b di siang hari

Kantor A mengakses CCTV kantor C



Gambar 9. (a), (b) Prview kantor Kelurahan Tangerang Selatan

Pada gambar 9 merupakan priview CCTV kantor B yang dapat di akses jarak jauh oleh kantor A. priview gambar 9 di ambil pada gambar di pagi hari, gambar b di siang hari

Pada tahapan ini memberikah hasil dari pengujian jaringan CCTV yang digunakan sebelumnya dan sudah diterapkan, dengan melalui pengujian QoS (Quality of Service), dimana perhitungan QoS ada throughput, packet loss, delay dan jitter.

TABEL VII  
HASIL PENGUIAN QOS SEBELEUM PENERAPAN

Indeks Parameteer <i>Jitter</i>		
Parameter	Hasil Perhitungan	Kategori
Throughput	8.8%	Buruk
Packet Loss	9,2%	Bagus
Delay	261,75 ms	Sedang
Jitter	260,75 ms	Buruk

TABEL VIII  
HASIL PENGUJIAN QOS SESUDAH PENERAPAN

Indeks Parameteer <i>Jitter</i>		
Parameter	Hasil Perhitungan	Kategori
Throughput	100%	Sangat Bagus
Packet Loss	0%	Sangat Bagus
Delay	82,5 ms	Sangat Bagus
Jitter	81,6 ms	Sedang

Dari hasil tabel pengujian parameter di atas, dapat dilihat perhitungan sebelum dan sesudah penerapan. Dimana setelah penerapan VPN tingkat keamanan dan ke stabilan jaringan yang meningkat pada *throughput*, *pecket loss*, *delay* maupun *jitter*.

#### IV. KESIMPULAN

Implementasi VPN menggunakan metode PPTP berhasil mengamankan koneksi antara kantor A (Kecamatan Bukit Raya) dengan kantor B (Kelurahan Tangkerang Selatan) dan kantor C (Kelurahan Simpang Tiga). Hal ini memungkinkan pihak kecamatan untuk mengakses data monitoring CCTV secara stabil dan mencegah akses oleh IP address di luar jaringan VPN. Konfigurasi VPN PPTP pada ketiga router menunjukkan keberhasilan, ditandai dengan stabilnya ping antar router antara kantor A, B, dan C. Dengan demikian, akses data CCTV secara jarak jauh dapat dilakukan dengan lancar. Hasil pengujian menunjukkan bahwa kantor A berhasil memantau CCTV di kantor B dan kantor C, memperkuat kemampuan akses data secara jarak jauh. Pengujian Quality of Service (QoS) menunjukkan peningkatan signifikan setelah penerapan VPN PPTP. Terdapat peningkatan throughput dengan selisih sekitar 90%, penurunan packet loss sebesar 9,2%, serta penurunan delay dan jitter dengan selisih sekitar 180 ms. Hal ini membuktikan bahwa VPN PPTP memiliki pengaruh besar terhadap kecepatan dan kestabilan jaringan, sehingga meningkatkan efisiensi operasional dan keamanan di Kecamatan Bukit Raya.

#### REFERENSI

- [1] F. Akbar, S. Susafa'ati, and M. Napiah, "Metode Point to Point Tunneling Protocol Untuk Keamanan Jaringan Studi Kasus Kantor Walikota Administrasi Jakarta Barat," *Jurnal Infortech*, vol. 1, no. 2, pp. 85–91, 2020, doi: 10.31294/infortech.v1i2.7112.
- [2] A. Tedyyana, O. Ghazali, and O. Purbo, "Model Design of Intrusion Detection System on Web Server Using Machine Learning Based," in *Proceedings of the 11th International Applied Business and Engineering Conference, ABEC 2023, September 21st, 2023, Bengkalis, Riau, Indonesia*, EAI, 2024. doi: 10.4108/eai.21-9-2023.2342879.
- [3] A. T. Atmoko, A. Surya Budiman, and N. Nuraeni, "Perancangan Dan Pengembangan Virtual Private Network (VPN) Menggunakan PPTP Pada PT Indobinatu Mitra Sejati Design and Development of Virtual Private Network (VPN) Using PPTP in PT Indobinatu Mitra Sejati," *Jtsi*, vol. 5, no. 1, pp. 160–170, 2024.
- [4] H. Supriyono, J. A. Widhaya, and A. Supardi, "Penerapan Jaringan VPN Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami," *Jarkom*, vol. 16, no. 2, pp. 88–101, 2013.
- [5] S. Sidik, S. Susafa'ati, E. R. Nainggolan, and U. Radiah, "Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board," *Jurnal Infortech*, vol. 3, no. 1, pp. 46–51, 2021, doi: 10.31294/infortech.v3i1.10400.

- [6] S. Watmah, "Implementasi VPN Menggunakan Point-To-Point Tunneling Protocol (PPTP) Mikrotik Router Pada BPRS Bumi Artha Sampang," *INSANTEK - Jurnal Inovasi dan Sains Teknik Elektro*, vol. 1, no. 1, pp. 6–12, 2020.
- [7] A. Tedyyana, O. Ghazali, and O. W. Purbo, "A real-time hypertext transfer protocol intrusion detection system on web server," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 3, p. 566, Jun. 2023, doi: 10.12928/telkomnika.v21i3.24938.
- [8] F. & L. M. Pratama, "Perancangan Jaringan Komputer Menggunakan Aplikasi Vhp Online Reporting System," *Jurnal Teknik Komputer Amik Bsi*, vol. 1, no. 1, pp. 106 & 107, 2015.
- [9] Y. N. Sari, D. Irfan, and A. Huda, "Network Security Analysis Using Virtual Private Network in Vocational School," *Jurnal Paedagogy*, vol. 9, no. 3, p. 582, 2022, doi: 10.33394/jp.v9i3.5346.
- [10] A. Amarudin and S. D. Riskiono, "Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn)," *Jurnal Teknoinfo*, vol. 13, no. 2, p. 100, 2019, doi: 10.33365/jti.v13i2.309.
- [11] 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," *Jurnal Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.
- [12] M. Rasuanda and Haeruddin, "Perbandingan Performa VPN Menggunakan PPTP Dan SSTP Over SSL Dengan Metode Quality of Service," *Journal of Information System and Technology*, vol. 01, no. 02, pp. 110–123, 2020.
- [13] W. K. Halawa and K. J. D. Lase, "Analisis Perbandingan Vpn Pptp Dan Eoip Menggunakan Metode Aqm," *INFACT : Jurnal Sains dan Komputer*, vol. 6, no. 1, pp. 39–48, 2021.
- [14] D. Gusrion, "Jurnal KomtekInfo," *Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko Muko*, vol. 5, no. 1, pp. 1–6, 2021.
- [15] S. T. Oktavia, D. F. Priambodo, N. Trianto, and R. Purwoko, "Comparative Quality of Service Analysis of VPN Protocols on IPv6," *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, vol. 12, no. 3, pp. 461–471, 2024, doi: 10.23887/janapati.v12i3.69264.
- [16] D. Dahnia, "Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik," *Jurnal Ilmiah Informatika Global*, vol. 10, no. 2, pp. 107–113, 2019, doi: 10.36982/jiig.v10i2.858.
- [17] D. N. Amadi, A. Budiman, and P. Utomo, "Analysis of the effectiveness of VPN and PPTP Protocol in E-Link Health Report Application Using NDLC Method," vol. 6, no. 2, pp. 949–958, 2024, doi: 10.51519/journalisi.v6i2.746.