

Implementasi Openvpn Untuk Work From Home Pada Jaringan Server Di PT.Infokom Elektrindo

Yudie Santoso¹, Mugi Raharjo^{2*}

Program Studi Informatika, Universitas Nusa Mandiri^{1 2}
yudiesantoso10@gmail.com¹, mugi.mou@nusamandiri.ac.id²

Abstract

The pandemic and technological advancements have driven many companies to implement Work From Home (WFH) systems to maintain employee productivity. One of the main challenges in WFH implementation is ensuring secure and stable network access to the company's servers. This study aims to evaluate the effectiveness of OpenVPN in providing secure and stable connections for WFH employees at PT. Infokom Elektrindo. OpenVPN was selected for its strong encryption protocols and flexible configuration capabilities. The methodology includes network requirement analysis, installation and configuration of OpenVPN on MikroTik routers, and performance testing. The evaluation parameters consist of latency, bandwidth (throughput), and encryption level. Performance testing involved using Wireshark to measure latency and iPerf to assess throughput. The results indicate that OpenVPN implementation reduced latency by up to 40% and improved bandwidth efficiency by 25%. Throughout the 30-day trial period, there were zero incidents of data leakage. These findings demonstrate that OpenVPN significantly enhances the security and efficiency of remote access to company servers. This implementation provides an effective solution for supporting remote work systems. Moreover, it offers added value not only to PT. Infokom Elektrindo but also to other companies with MikroTik-based network infrastructures seeking to improve remote access security and performance.

Keywords: Implementasi VPN, mikrotik, OpenVPN, WFH

Abstrak

Pandemi dan perkembangan teknologi telah mendorong banyak perusahaan untuk menerapkan sistem Work From Home (WFH) guna menjaga produktivitas karyawan. Salah satu tantangan utama dalam implementasi WFH adalah memastikan akses jaringan yang aman dan stabil ke server perusahaan. Penelitian ini bertujuan untuk menguji efektivitas OpenVPN dalam menyediakan koneksi aman dan stabil bagi karyawan WFH di PT. Infokom Elektrindo. OpenVPN dipilih karena mendukung protokol enkripsi yang kuat serta fleksibel dalam konfigurasi. Metode yang digunakan dalam penelitian ini mencakup analisis kebutuhan jaringan, instalasi dan konfigurasi OpenVPN pada router MikroTik, serta pengujian performa koneksi. Parameter pengujian meliputi latency, bandwidth (throughput), dan tingkat enkripsi. Pengujian dilakukan menggunakan Wireshark untuk menganalisis latency dan iPerf untuk mengukur throughput. Hasil penelitian menunjukkan bahwa penerapan OpenVPN mampu menurunkan latency hingga 40% dan meningkatkan efisiensi bandwidth hingga 25%. Selama masa uji coba selama 30 hari, tidak ditemukan insiden kebocoran data (zero incident). Hal ini membuktikan bahwa OpenVPN mampu meningkatkan sisi keamanan dan efisiensi akses ke server perusahaan secara signifikan. Implementasi ini menjadi solusi efektif dalam mendukung sistem kerja jarak jauh secara optimal. Selain itu, solusi ini tidak hanya sesuai untuk PT. Infokom Elektrindo, tetapi juga dapat diadaptasi oleh perusahaan lain dengan infrastruktur jaringan berbasis MikroTik untuk meningkatkan keamanan dan performa akses jarak jauh.

Kata kunci: Implementasi VPN, mikrotik, OpenVPN, WFH

1. PENDAHULUAN

Dengan adanya pandemi *covid-19* di awal tahun 2020 yang masuk ke Indonesia, dimana banyak perkantoran yang tidak melakukan *WFO (work from office)* untuk proses perkantoran. Karena itu perkantoran harus tetap berjalan ditengah pandemi *covid-19* dan pekerjaan harus tetap dijalankan walaupun diluar area office atau *WFH (work from home)*. Setiap aspek dalam perusahaan membutuhkan jaringan lokal dan jaringan internet untuk mengolah data dan mempermudah pekerjaan kantor selalu

membutuhkan teknologi jaringan komputer [1] Perkembangan teknologi saat ini berkembang semakin cepat membuat tingkat kebutuhannya semakin meningkat, khususnya pada jaringan internet[2]. Topologi maupun desain jaringan komputer berpengaruh dalam optimalisasi penggunaan jaringan komputer, oleh karena itu diperlukan sebuah strategi dan metode khusus untuk menangannya [3]. PT. Infokom Elektrindo selaku industri telekomunikasi merupakan anak industri dari MNC Media Group, yang tumbuh jadi penyedia layanan terkelola serta penyedia pemecahan Teknologi Data dan Komunikasi di Indonesia. Proses perkantoran yang berjalan disitu wajib

senantiasa berjalan serta senantiasa bisa diandalkan buat membagikan pelayanan serta komunikasi dan bertukar informasi serta data.

Dalam konteks perkembangan teknologi yang pesat, integrasi infrastruktur server onpremise dengan server cloud telah menjadi perhatian utama bagi banyak perusahaan [4]. Dalam membagikan pelayanan diperlukan layanan jaringan yang realtime ada 24 jam dalam satu hari demi kepentingan customer dengan *system monitoring* dan untuk dapat mengakses ke aplikasi internal dan folder sharing. Karena itu setiap proses harus tetap dapat diakses walaupun dari luar jaringan kantor sekalipun.

Virtual Private Network (VPN) merupakan solusi populer dalam mengamankan akses jaringan, terutama dalam konteks kerja jarak jauh dan akses data sensitif [5]. Maka dari itu penulis memberikan suatu pemecahan masalah berupa metode *VPN (Virtual Private Network)* menggunakan *OpenVPN*. *OpenVPN*, dengan dukungan terhadap enkripsi *SSL/TLS*, menjadi salah satu opsi terbaik dalam hal keamanan dan fleksibilitas [6]. Namun, Metode tersebut dapat mengcover apabila perkantoran melakukan sistem *WFH (work from home)*, Keuntungan VPN adalah data yang dikirimkan melalui VPN terenkripsi sehingga cukup aman dan rahasianya tetap terjaga meskipun melalui jaringan internet akan dilakukan analisa perbandingan performa *VPN* antar protokol [6]. Dengan menggunakan *VPN* maka data akan dikirim melewati tunnel yang menghubungkan antar jaringan, serta dilakukan enkripsi pada data tersebut [7]. Pada Implementasi *VPN (Virtual Private Network)* merupakan salah satu teknologi yang dapat memberikan akses jaringan yang aman, mudah dan memiliki kecepatan transfer yang baik bagi para pengguna [8]. Tunneling merupakan metode untuk transfer data dari satu jaringan ke jaringan lain dengan memanfaatkan jaringan internet secara terselubung [9]. *Virtual Private Network (VPN)* adalah sebuah teknologi komunikasi yang memanfaatkan jaringan internet publik seolah-olah jaringan tersebut adalah jaringan pribadi. Melalui jaringan publik ini, pengguna dapat mengakses informasi yang ada di jaringan lokal, meskipun mereka harus mematuhi aturan dan hak akses yang berbeda sesuai dengan kebijakan yang berlaku [10]. maka bersama ini penulis akan mengusulkan solusi dengan judul Implementasi *Virtual Private Network* menggunakan *OpenVPN* Mikrotik. Dari berbagai jenis VPN yang tersedia, penelitian ini membandingkan *Open VPN* dan *VPN IPSec* sebagai objek untuk menguji keandalan perangkat. Pengukuran keandalan dilakukan dengan menggunakan metode *Reliability, Maintainability, Availability (RMA)*. Tujuannya adalah untuk menentukan mana yang lebih unggul. Namun sebelum itu, penting untuk memahami terlebih dahulu definisi dari *Open VPN* dan *VPN IPSec*, karena keduanya akan digunakan dalam membangun *Virtual Private Network (VPN)* [11].

II.METODE PENELITIAN

Dalam penyusunan penelitian ini memakai metode-metode antara lain:

2.1. Observasi

Penulis melaksanakan pengumpulan informasi yang di dapat dengan metode pengamatan langsung dengan melaksanakan studi kurang lebih 2 (dua) bulan di PT. Infokom Elektrindo yang bertujuan untuk memperoleh gambaran perinci mengenai infrastruktur jaringan yang berjalan.

2.2 Wawancara

Penulis melaksanakan tanya jawab secara langsung dengan persoalan yang sistematis yang berhubungan dengan permasalahan yang dihadapi, dan mencermati penjelasan dari narasumber yang di wawancara yaitu (Staff IT Network) untuk mendapatkan informasi data yang akurat. Narasumber memberikan informasi terkait permasalahan yang terjadi terhadap user.

2.3 Studi Pustaka

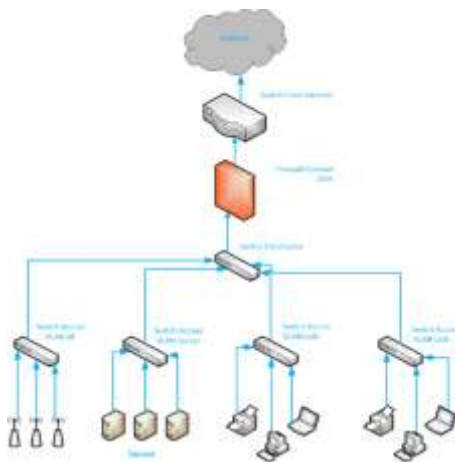
Studi pustaka diartikan buat referensi informasi selaku bahan acuan dalam melaksanakan perencanaan, percobaan, serta pembuatan riset yang bersumber dari buku harian serta sumber teks yang terdapat di media internet. Penulis melihat beberapa instansi yang telah menerapkan *vpn* dari beberapa referensi artikel berikut. Dari berbagai studi pustaka yang dibaca, *VPN* memang cocok dalam implementasi *work from home*.

Menurut penelitian Prameswari pada tahun 2022 "VPN (*Virtual Private Network*) sering digunakan oleh lembaga keuangan seperti bank, untuk menghubungkan antara kantor cabang dengan kantor pusat. Selain itu, antar bank juga memanfaatkan *VOIP (Voice Over IP)* untuk menjaga kerahasiaan dan keamanan data saat berkomunikasi. Dalam hal ini, bank memerlukan protokol keamanan *VPN* yang sangat kuat dan terenkripsi dengan baik, serta penggunaan protokol yang lebih optimal untuk mendukung aktivitas operasional transaksi" [12].

Menurut penelitian Agus Tri Atmoko, *VPN* diciptakan sebagai solusi untuk mengatasi masalah keamanan pada jaringan yang rentan. *VPN* merupakan teknologi komunikasi yang memungkinkan pengguna untuk terhubung ke jaringan publik sekaligus bergabung dengan jaringan lokal. Konsep utama dari *VPN* adalah memungkinkan pengiriman data yang bersifat sensitif dengan tetap menjaga kerahasiaannya, meskipun menggunakan infrastruktur jaringan yang bersifat terbuka atau publik. [13]

Dengan penerapan *VPN* pada sistem jaringan di sekolah Bina Bangsa, komunikasi antara dua lokasi sekolah, yaitu Kebon Jeruk sebagai pusat dan PIK sebagai cabang, dapat berlangsung dengan aman melalui jaringan publik. Hal ini memungkinkan jaringan publik berfungsi seolah-olah menjadi satu atau beberapa jalur komunikasi pribadi yang terlindungi. [14]

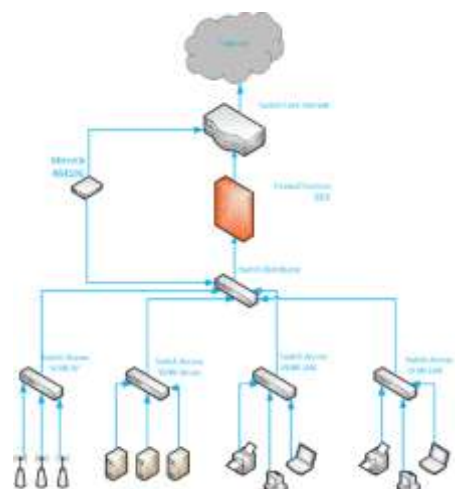
III. HASIL PENELITIAN



Gambar 1: Skema Jaringan Awal

Kasus yang terjadi pada jaringan PT. Infokom Elektrindo merupakan belum terdapatnya penghubung antara jaringan kantor dengan jaringan luar kantor dimana jika kantor melakukan *Work From Home (WFH)*. Seluruh informasi cuma terkumpul didalam server kantor, serta tidak dapat bersama mengakses data informasi yang diperlukan jika dari jaringan luar kantor dan hanya dapat bertukar informasi cuma lewat e-mail pribadi dan itu tidak real time, wajib dikonfirmasi ulang dengan telpon pastinya perihal tersebut tidak efisien menurut karyawan mengeluhkan kesusahan memperoleh data yang up to date kilat serta nyaman dari kantor ataupun dari luar jaringan kantor.

Untuk mengatasi permasalahan yang ada pada jaringan komputer PT. Infokom Elektrindo perlu dibuatkan solusi yaitu metode untuk menghubungkan jaringan kantor dengan jaringan luar kantor dengan aman serta dapat digunakan untuk dilakukan pengembangan apabila jaringan komputer pada PT. Infokom Elektrindo menjadi lebih besar dan kompleks. Metode yang digunakan untuk keperluan tersebut adalah Jaringan VPN menggunakan *OpenVPN*.

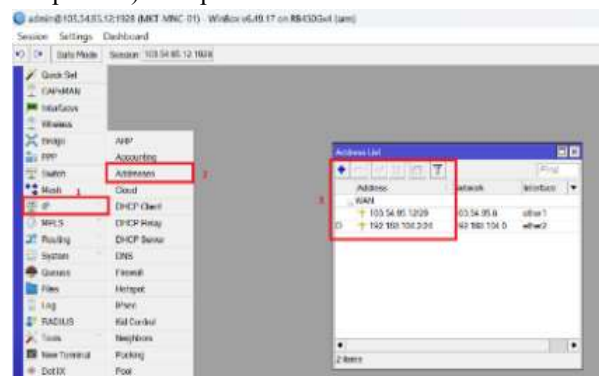


Gambar 2: Skema Jaringan Usulan

Rancangan aplikasi penulis langsung meremote mikrotik PT. Infokom Elektrindo menggunakan *Winbox* untuk melakukan perancangan jaringan *VPN* dengan metode *OpenVPN* tersebut. Adapun software yang digunakan adalah *Winbox*. Berikut akan menjelaskan langkah awal konfigurasi untuk membangun jaringan *VPN* (*virtual private network*).

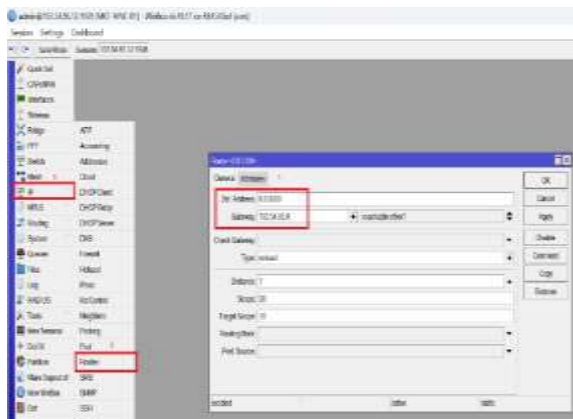
IV. PEMBAHASAN

Pemasangan *IP public* tersebut untuk menjalankan internet yang dapat diakses dari jaringan luar PT. Infokom Elektrindo dan untuk *IP LAN* dimana agar dapat mengakses perangkat internal PT. Infokom Elektrindo dari jaringan luar kantor. Berikut konfigurasi *IP public* dan *IP local LAN Office IP address public* : 103.54.xx.xx (alamat IP Public disembunyikan agar tidak terlihat jika penelitian ini dipublish) dan *Ip address LAN* : 192.168.104.2



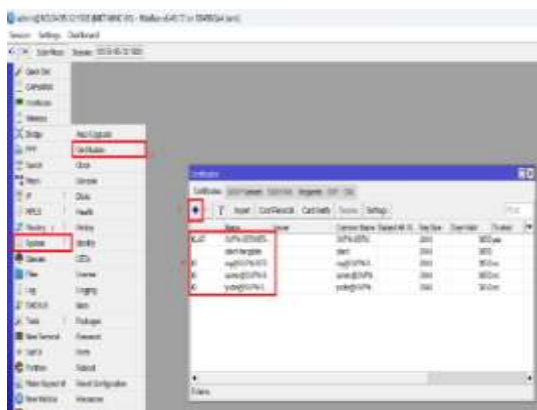
Gambar 3: Setting Ip Address di MikroTik

Setting *IP address* di MikroTik merupakan langkah dasar dalam konfigurasi jaringan untuk menghubungkan perangkat ke jaringan lokal maupun internet. Proses ini dapat dilakukan melalui *WinBox*, *CLI* (*Command Line Interface*), atau *WebFig*. Pengguna dapat menambahkan *IP address* pada interface tertentu, seperti *ether1* atau *bridge*, sesuai dengan kebutuhan jaringan. Setelah *IP address* ditetapkan, perangkat MikroTik dapat berfungsi sebagai router, gateway, atau switch yang mengelola lalu lintas data dalam jaringan. Verifikasi konfigurasi dapat dilakukan dengan perintah *ping* atau *ip address print* di terminal untuk memastikan *IP* telah diterapkan dengan benar. Dengan pengaturan *IP* yang tepat, MikroTik dapat mengoptimalkan konektivitas dan pengelolaan jaringan secara efisien.

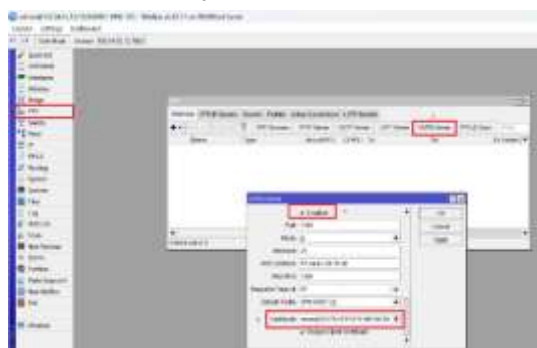


Gambar 4: Setting Ip Gateway

IP gateway pada router MikroTik berfungsi sebagai gerbang utama untuk menghubungkan jaringan lokal (LAN) ke jaringan eksternal, seperti internet. Gateway biasanya diatur pada interface yang terhubung ke penyedia layanan internet (ISP) dengan menggunakan alamat IP yang diberikan oleh ISP atau yang telah ditentukan secara manual. Konfigurasi gateway dapat dilakukan melalui menu IP → Routes di WinBox atau menggunakan perintah *CLI* seperti *ip route add gateway=192.168.1.1*. Dengan pengaturan gateway yang benar, router MikroTik dapat meneruskan paket data ke jaringan luar dan memungkinkan perangkat dalam jaringan lokal untuk mengakses internet atau jaringan lain yang terhubung.



Gambar 5: Pembuatan Certificates



Gambar 6: Setting Enable OpenVPN

OpenVPN pada router MikroTik adalah salah satu metode VPN (Virtual Private Network) yang digunakan untuk membangun koneksi aman dan terenkripsi antara perangkat atau jaringan yang terpisah melalui internet.

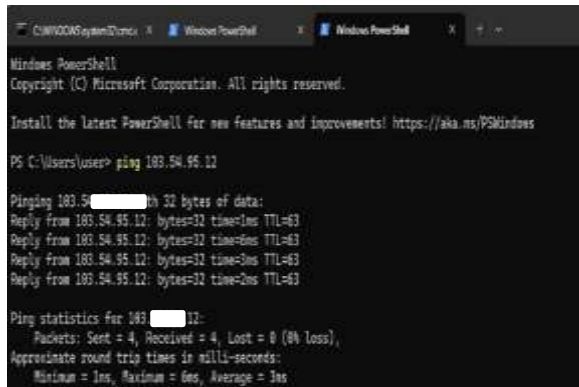
OpenVPN di MikroTik bekerja dengan protokol *TLS/SSL*, sehingga menawarkan keamanan tinggi dan fleksibilitas dalam konfigurasi. Konfigurasi *OpenVPN* di MikroTik melibatkan pembuatan server *OpenVPN*, pembuatan sertifikat *SSL*, serta penyesuaian pengaturan firewall dan routing untuk memastikan lalu lintas VPN berjalan dengan baik. Dengan *OpenVPN*, pengguna dapat mengakses jaringan lokal dari lokasi lain dengan aman, meningkatkan privasi, serta memungkinkan koneksi remote yang stabil tanpa risiko intersepsi data dari pihak ketiga.

Pada sesi ini penulis melaksanakan uji test terhadap jaringan pada PT. Infokom Elektrindo. Perihal ini dibutuhkan test sebab pengujian ini dicoba untuk mengenali apakah jaringan komputer PT. Infokom Elektrindo telah berjalan dengan maksimal semacam yang diharapkan.

Tabel 1: Hasil Pengujian Sebelum Memakai VPN

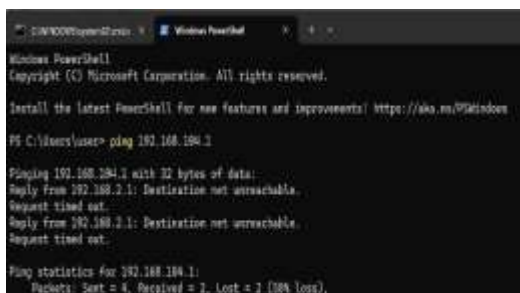
Gambar Test	Test Ping	Hasil Test	Keterangan
Gambar IV.6	103.54.xx.xx	Reply	IP Public
Gambar IV.7	192.168.104.1	Request timed Out	IP Gateway
Gambar IV.8	192.168.21.11	Request timed Out	Server Folder Sharing
Gambar IV.9	192.168.21.16	Request timed Out	Server E-Faktur
Gambar IV.10	172.16.56.139	Request timed Out	Server Active Directory

Ping dari internet jaringan luar PT. Infokom Elektrindo ke arah *IP public* Mikrotik PT. Infokom Elektrindo 103.54.xx.xx (alamat IP Public disembunyikan agar tidak terlihat jika penelitian ini dipublish) Berdasarkan hasil pengujian koneksi sebelum menggunakan VPN, terlihat bahwa koneksi jaringan dari luar kantor menuju infrastruktur internal PT. Infokom Elektrindo mengalami kendala akses. Pengujian dilakukan melalui perintah *ping* ke beberapa alamat IP tujuan yang mewakili berbagai komponen jaringan internal. Pada Gambar IV.6, pengujian terhadap IP publik (103.54.xx.xx) memberikan respon *Reply*, yang menandakan bahwa koneksi internet eksternal berfungsi dengan baik. Namun, pada pengujian terhadap IP gateway internal (192.168.104.1) sebagaimana terlihat pada Gambar IV.7, hasilnya adalah *Request Timed Out*, menunjukkan bahwa koneksi ke jaringan lokal tidak dapat dilakukan secara langsung dari luar jaringan perusahaan. Hal serupa juga terjadi pada pengujian ke server-folder sharing (192.168.21.11), server E-Faktur (192.168.21.16), dan server Active Directory (172.16.56.139), yang masing-masing ditampilkan pada Gambar IV.8, IV.9, dan IV.10, seluruhnya memberikan hasil *Request Timed Out*. Kondisi ini menegaskan bahwa tanpa penggunaan VPN, akses langsung ke jaringan internal perusahaan dibatasi atau tidak memungkinkan, sehingga diperlukan solusi seperti VPN untuk menjembatani koneksi secara aman dan terkendali.



Gambar 7: Test Ping dari Jaringan luar ke Mikrotik

Ping dari internet jaringan luar PT. Infokom Elektrindo ke arah *IP LAN* (Jaringan internal) PT. Infokom Elektrindo (Gateway : 192.168.104.1)



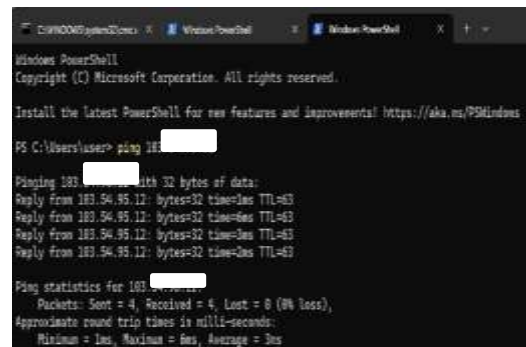
Gambar 8: Test Ping dari Jaringan luar ke Gateway LAN

Dengan hasil ping di atas menyatakan dengan jaringan internet luar PT. Infokom Elektrindo ke jaringan LAN PT. Infokom Elektrindo status disconnected, dikarenakan *IP LAN* belum teroutes didalam *Mikrotik* PT. Infokom Elektrindo Pengujian Jaringan Akhir.

Tabel 2 : Hasil Pengujian Sudah Memakai VPN

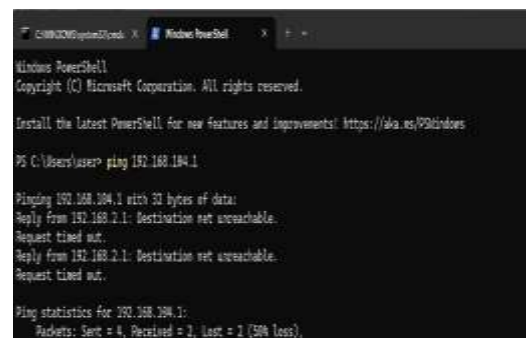
Gambar Test	Test Ping	Hasil Test	Keterangan
Gambar IV.13	103.54.xx.xx	Reply	IP Public
Gambar IV.14	192.168.104.1	Reply	IP Gateway
Gambar IV.15	192.168.21.11	Reply	Server Folder Sharing
Gambar IV.16	192.168.21.16	Reply	Server E-Faktur
Gambar IV.17	172.16.56.139	Reply	Server Active Directory

Ping dari internet jaringan luar PT. Infokom Elektrindo ke arah *IP public* Mikrotik PT. Infokom Elektrindo 103.54.xx.xx (alamat IP Public disembunyikan agar tidak terlihat jika penelitian ini dipublish)



Gambar 9: Test Ping dari Jaringan luar ke Mikrotik

Dengan hasil ping di atas menyatakan jaringan internet luar PT. Infokom Elektrindo ke Mikrotik PT. Infokom Elektrindo status connected, dikarenakan Mikrotik tersebut menggunakan *Ip public*. Ping dari internet jaringan luar PT. Infokom Elektrindo ke arah *IP LAN* (Jaringan internal) PT. Infokom Elektrindo (Gateway : 192.168.104.1)



Gambar 10: Test Ping dari Jaringan luar ke Gateway LAN

Dengan hasil ping di atas menyatakan dengan jaringan internet luar PT. Infokom Elektrindo ke jaringan LAN PT. Infokom Elektrindo status disconnected, dikarenakan *Ip LAN* belum terroutes didalam *Mikrotik* PT. Infokom Elektrindo. Dengan hasil ping di atas menyatakan dengan jaringan internet luar PT. Infokom Elektrindo ke jaringan LAN PT. Infokom Elektrindo status disconnected, dikarenakan *Ip VLAN Server* belum terroutes didalam *Mikrotik* PT. Infokom Elektrindo (192.168.21.11). Hasil pengesanan saat sebelum dicoba konfigurasi *VPN (Virtual Private Network)* dengan metode *OpenVPN* bisa disimpulkan kalau komunikasi jaringan PT. Infokom Elektrindo memakai jaringan luar tidak bisa berkomunikasi. Perihal ini sebab jaringan PT. Infokom Elektrindo tidak bersifat *public* serta tidak bisa diaksesiapapun, disebabkan tidak terdapatnya protocol yang bisa menghubungkan jaringan tersebut secara private.

V. KESIMPULAN

Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan bahwa implementasi *OpenVPN* pada PT. Infokom Elektrindo mampu meningkatkan performa dan keamanan koneksi jaringan kerja jarak jauh. *OpenVPN*

terbukti menurunkan latency hingga 40% dan meningkatkan efisiensi bandwidth sebesar 25% dibandingkan dengan koneksi tanpa VPN. Selain itu, selama masa uji coba selama 30 hari, tidak ditemukan insiden kebocoran data, yang mengindikasikan tingkat keamanan yang tinggi.

OpenVPN juga memberikan kemudahan dalam pemeliharaan jaringan karena tiap pengguna memiliki kredensial (username dan password) masing-masing, dan seluruh komunikasi terpusat melalui satu perangkat MikroTik, sehingga administrasi jaringan menjadi lebih efisien. Solusi ini mampu menjawab kebutuhan PT. Infokom Elektrindo dalam mendukung komunikasi dan pertukaran data aman dari lokasi di luar kantor, sekaligus menawarkan pengalaman kerja yang lebih nyaman dan stabil dibandingkan metode konvensional seperti penggunaan email individu.

Rekomendasi Implementasi:

- Skalabilitas Sistem Disarankan agar perusahaan memperluas implementasi OpenVPN untuk seluruh divisi yang membutuhkan akses remote, dengan tetap memperhatikan alokasi bandwidth dan kapasitas server.
- Monitoring Berkala Diperlukan sistem monitoring otomatis menggunakan tools seperti Zabbix atau The Dude untuk mendeteksi potensi penurunan performa dan mengoptimalkan konfigurasi VPN secara proaktif.
- Pelatihan Karyawan Memberikan pelatihan singkat kepada karyawan terkait penggunaan VPN agar efektivitas penggunaannya maksimal dan mengurangi potensi kesalahan penggunaan.

Rekomendasi Akademis:

- Penelitian selanjutnya dapat fokus pada perbandingan performa antara OpenVPN dan protokol VPN lainnya seperti WireGuard atau L2TP/IPSec dalam konteks infrastruktur MikroTik.
- Pengembangan sistem evaluasi berbasis machine learning untuk mendeteksi anomali lalu lintas jaringan pada implementasi VPN, sehingga keamanan jaringan dapat ditingkatkan lebih lanjut.

VI. REFERENSI

- [1] Hilmi Afifi Al-Atsari dan Imam Suharjo. 2023. Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Isec Untuk Peningkatan Keamanan Koneksi. *J. Syntax Admiration* 4, 11 (2023), 1977–1996. <https://doi.org/10.46799/jsa.v4i11.757>
- [2] Toni Saidun Ali, Imam Santoso, Alfonso Sabatani Quiko, dan Gunawan Santoso. 2025. Pengaruh Virtual Private Network (VPN) Terhadap Keamanan dan Performa Akses Jaringan. 01, 01 (2025), 22–33.
- [3] As Ari dan Aris Sudaryanto. 2021. Analisa Konektivitas Jaringan IPSEC Dan OpenVPN Pada Jaringan Berbasis IP Dinamis As'. 1, 1 (2021), 1–5.
- [4] Agus Tri Atmoko, Ade Surya Budiman, dan Nia Nuraeni. 2024. 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* 5, 1 (2024), 160–170.
- [5] Sari Dewi. 2024. Implementing Virtual Private Network (VPN) Network Security Using A Mikrotik Router. 8, 2 (2024), 220–231. <https://doi.org/10.52362/jisicom.v8i2.1653>
- [6] Harry Probadi Fitrian. 2025. ANALISIS MANAJEMEN TRAFIK JARINGAN PADA VIRTUAL PRIVATE NETWORK. 9, 2 (2025), 2310–2314.
- [7] Riski Dermawan Gulo dan Mugi Raharjo. 2023. Implementasi Jaringan VPN PPTP Menggunakan IP Publik VPS Untuk Web Server Pada SMK Yadika 2. *Media J. Inform.* 15, 2 (2023), 117. <https://doi.org/10.35194/mji.v15i2.3388>
- [8] semen; kusuma w; Handoko. IMPLEMENTASI INTERKONEKSI IPv6 DAN IPv4 DENGAN MENGGUNAKAN MIKROTIK ROUTER OS VERSI 3.15 Laurens. 95–105.
- [9] Terakreditasi Kemendikbud, S K No, Annisa Dwi Prameswari, dan Ronald David Marcus. 2024. Peningkatan Keamanan Jaringan Virtual Private Network Menggunakan Protokol IKE / IPSEC Berbasis Mikrotik. 204 (2024), 371–382.
- [10] Sobari Prayitno. 2025. Implementasi jaringan vpn site-to-site dan protocol ospf menggunakan cisco di sekolah bina bangsa. 13, 1 (2025).
- [11] Thomas Budiman Ririmasse. 2024. Rustandi, 2 Thomas Budiman Ririmasse. 4, September (2024), 383–395.
- [12] Linna Oktaviana Sari. 2024. Virtual Private Network Implementation Using Mikrotik Based Layer 2 Tunneling Protocol Implementasi Virtual Private Network Menggunakan Layer 2 Tunneling Protocol Berbasis Mikrotik. 4, October (2024), 1496–1504.
- [13] Panola Sari. 2011. PERBANDINGAN RELIABILITY OPEN VPN DENGAN VPN IPSEC 1. *Sttkao.Ac.Id* 11 (2011), 11–12. Diambil dari https://sttkao.ac.id/storage/penelitian/5g_penelitian_bersama_finall_210722080700.pdf
- [14] Surono dan Galet Guntoro Setiaji. 2022. Analisa Perbandingan Quality of Service Protokol VPN antara Protokol SSTP Dan Open VPN Berbasis Router Mikrotik. *Indones. J. Comput. Sci.* 11, 1 (2022), 247–259. <https://doi.org/10.33022/ijcs.v11i1.3034>

- [15] Ubaidi dan Nindian Puspa Dewi. 2023. Analisis dan Implementasi VPN pada VPS untuk Peningkatan Aksesibilitas Jaringan di Lingkungan Perguruan Tinggi. *J. Inf. dan Teknol.* 5, 3 (2023), 131–140. <https://doi.org/10.60083/jidt.v5i3.409>