

**IMPLEMENTASI DAN ANALISIS JARINGAN VPN
MENGUNAKAN OPENVPN PADA JARINGAN LOKAL
(Studi Kasus: Kantor Desa Tumbang Nusa)**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada program studi ilmu komputer



diajukan oleh

Destri Ratna Sari

NIM 19.53.021338

**PROGRAM STUDI ILMU KOMPUTER
FAKULTAS BISNIS DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH PALANGKARAYA
2025**

INTISARI

Keamanan dan ketersediaan akses data merupakan kebutuhan penting dalam pengelolaan jaringan pada instansi pemerintahan, termasuk pada Kantor Desa Tumbang Nusa. Untuk memenuhi kebutuhan tersebut, penelitian ini bertujuan mengimplementasikan dan menganalisis kinerja jaringan Virtual Private Network (VPN) menggunakan OpenVPN pada jaringan lokal kantor desa. Metode penelitian yang digunakan meliputi observasi langsung, pengujian jaringan, serta analisis konfigurasi OpenVPN pada server dan klien. Penelitian juga mengevaluasi performa jaringan sebelum dan sesudah implementasi VPN, dengan fokus pada aspek latensi, stabilitas koneksi, serta penggunaan bandwidth.

Hasil penelitian menunjukkan bahwa proses implementasi OpenVPN dapat dilakukan secara sistematis melalui instalasi server VPN, pembuatan sertifikat keamanan, konfigurasi routing, serta pengaturan klien. Dari sisi kinerja, penggunaan OpenVPN menambah latensi sekitar 10–20 ms akibat proses enkripsi, namun masih berada dalam batas normal dan tidak mengganggu aktivitas kerja pegawai. Stabilitas koneksi dinilai baik, ditunjang fitur auto-reconnect yang menjaga koneksi tetap aktif meskipun jaringan internet mengalami fluktuasi. Selain itu, OpenVPN terbukti meningkatkan keamanan dan fleksibilitas akses data, terutama untuk kebutuhan kerja jarak jauh.

Penelitian juga mengidentifikasi beberapa kelebihan OpenVPN, antara lain keamanan tinggi, bersifat open-source, kompatibilitas luas, serta dukungan autentikasi berbasis sertifikat. Namun, kekurangan seperti kebutuhan kemampuan teknis, ketergantungan pada kualitas internet, dan potensi peningkatan latensi tetap perlu diperhatikan. Secara keseluruhan, OpenVPN terbukti efektif sebagai solusi keamanan jaringan dan akses data jarak jauh bagi instansi berskala kecil hingga menengah seperti kantor desa.

Kata kunci: OpenVPN, VPN, Keamanan Jaringan, Jaringan Lokal, Akses Jarak Jauh, Enkripsi Data.

ABSTRACT

This research analyzes the implementation and performance of a Virtual Private Network (VPN) using OpenVPN on the local network of the Tumbang Nusa Village Office. The purpose of this study is to examine how OpenVPN is implemented in a local environment, evaluate the performance of the network before and after the use of VPN, and identify the advantages and disadvantages of OpenVPN in supporting secure remote access for village administrative operations. The study uses a descriptive qualitative approach supported by technical testing of latency, bandwidth usage, and connection stability.

The results show that the implementation of OpenVPN can be carried out effectively using a certificate-based authentication system, AES-256-GCM encryption, and TLS security mechanisms. Network performance testing indicates a slight increase in latency due to encryption overhead, but overall network performance remains stable and acceptable for operational needs. The main advantages of OpenVPN include strong security, compatibility with multiple devices, and the ability to provide secure remote access for employees. However, challenges arise related to technical knowledge, internet stability, and the need for comprehensive documentation.

This research contributes to the understanding of VPN application in small-scale government environments and provides recommendations for improving infrastructure and technical capacity. Future research is suggested to explore comparative performance between various VPN protocols or to implement multi-factor authentication for enhanced security.

Keywords: OpenVPN, VPN Security, Network Performance, Remote Access, Local Network Implementation.

DAFTAR ISI

INTISARI	i
<i>ABSTRACT</i>	ii
DAFTAR ISI	iii
DAFTAR TABEL.....	v
DAFTAR GAMBAR	vi
DAFTAR LAMPIRAN	vii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan	7
BAB II LANDASAN TEORI.....	10
2.1 Konsep Dasar Jaringan Komputer dan Keamanan	10
2.2 <i>Virtual Private Network (VPN)</i>	19
2.3 OpenVPN Arsitektur dan Komponen	24
2.4 Kriptografi pada OpenVPN.....	25
2.5 Aspek Kinerja UDP vs TCP, MTU/MSS, dan Kompresi	26
2.6 Parameter Pengukuran Kinerja.....	29
2.7 Penguatan (Hardening) dan Operasional.....	30
BAB III ANALISIS DAN PERANCANGAN SISTEM.....	33
3.1 Tinjauan Umum.....	33
3.2 Analisis Sistem	34
3.3 Perancangan Sistem	36
3.4 Rencana Implementasi	37
3.5 Kriteria Keberhasilan Sistem.....	37
BAB IV IMPLEMENTASI DAN PEMBAHASAN	39
4.1 Implementasi	39
4.2 Pembahasan	59
BAB V PENUTUP.....	68

5.1	Kesimpulan.....	DAFTAR ISI	68
5.2	Saran		69
	DAFTAR PUSTAKA		70
	LAMPIRAN		72

DAFTAR ISI

DAFTAR TABEL

Tabel 4.1 Konfigurasi port forwarding pada router TP-Link Archer.....	47
Tabel 4.2 Kendala terhadap Operasional dan Solusi	59

DAFTAR GAMBAR

Gambar 4.1 Instalasi Paket OpenVPN dan EasyRSA.....	44
Gambar 4.2 Pembuatan Certificate Authority	44
Gambar 4.3 Pembuatan Sertifikat Server	45
Gambar 4.4 Pembuatan Sertifikat dan Key Client.....	45
Gambar 4.5 Mengaktifkan IP Forwarding.....	46
Gambar 4.6 Menjalankan Layanan OpenVPN	46
Gambar 4.7 Pengujian Ping Antar Perangkat di Dalam VPN	49

DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi Server OpenVPN (server.conf)

Lampiran 2 Konfigurasi Client OpenVPN (client.ovpn)

Lampiran 3 Hasil Pengujian Kinerja Jaringan

Lampiran 4 Topologi Jaringan Implementasi

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat saat ini mendorong berbagai institusi, baik pendidikan, bisnis, maupun pemerintahan, untuk memanfaatkan jaringan komputer dalam mendukung aktivitas harian. Salah satu jenis jaringan yang paling umum digunakan adalah jaringan lokal (*Local Area Network / LAN*), yang memungkinkan perangkat di dalam suatu lokasi terbatas, seperti laboratorium, kantor, atau warnet, untuk saling terhubung dan bertukar data. Dalam konteks ini, keamanan data menjadi kebutuhan penting guna memastikan kelancaran komunikasi dan perlindungan terhadap informasi yang bersifat rahasia.¹

Saat ini kebutuhan akan koneksi jaringan yang aman dan andal di lingkungan organisasi baik kampus, pemerintahan, maupun perusahaan terus meningkat pesat. Hal ini dipicu oleh tiga hal utama yaitu kerja *hibrida/remote* yang menuntut akses jarak jauh ke sumber daya lokal (*file server*, aplikasi internal), meningkatnya ancaman keamanan siber, dan kebutuhan efisiensi biaya tanpa mengorbankan keamanan. *Virtual Private Network* (VPN) menjadi solusi yang umum dipakai karena mampu membentuk “terowongan” terenkripsi di atas jaringan publik agar lalu lintas data internal tetap privat.²

¹ Hafid, A., & Ardiansyah, A. (2021). Implementasi OpenVPN pada Infrastruktur Jaringan Virtualisasi Cloud Computing. *Jurnal Teknologi dan Sistem Komputer*, 9(2), 123-130.

² DemandSage. (2025). VPN Statistics of 2025: Usage, Market & Trends. Diakses 20 Agustus 2025

Data survei dan ulasan pasar terbaru menunjukkan penggunaan VPN baik untuk keperluan personal maupun kerja terus tumbuh dan menjadi kebiasaan harian bagi sebagian pengguna internet di berbagai negara. Fakta ini memperlihatkan bahwa VPN bukan lagi teknologi pelengkap, melainkan komponen inti dalam arsitektur jaringan modern.³

Berbagai implementasi VPN (seperti IPsec, L2TP, WireGuard), OpenVPN menempati posisi istimewa karena bersifat *open-source*, fleksibel, lintas platform, dan telah matang secara ekosistem. Sejak rilis mayor 2.6 pada Maret 2023, OpenVPN mengadopsi standar kriptografi yang lebih modern, mendukung OpenSSL 3.0, dan secara default mendorong penggunaan cipher AEAD seperti AES-256-GCM dan ChaCha20-Poly1305. Pembaruan ini relevan untuk organisasi yang ingin memastikan kesesuaian dengan praktik keamanan terkini sambil mempertahankan kompatibilitas dengan infrastruktur yang sudah ada.⁴

Namun, sebelum teknologi ini diadopsi secara luas, perlu dilakukan uji coba penerapan OpenVPN dalam jaringan lokal, misalnya di lingkungan kampus, laboratorium, atau warnet. Uji coba ini penting untuk melihat bagaimana pengaruh OpenVPN terhadap performa jaringan, kemudahan implementasi, serta dampaknya terhadap tingkat keamanan data. Dengan demikian, hasil dari penelitian ini diharapkan dapat menjadi referensi dalam memilih dan menerapkan sistem keamanan jaringan yang efektif dan efisien. Meski OpenVPN populer dan relatif mudah diterapkan, implementasi pada jaringan lokal (LAN) sering menghadapi

³ Security.org. (2025). Research Into VPN Usage (Updated Statistics). Diakses 20 Agustus 2025.

⁴ Exploding Topics. (2024). VPN Statistics, Trends & Facts. Diakses 20 Agustus 2025.

kendala diantaranya yaitu Desain topologi dan mode koneksi, Keamanan kriptografi dan kepatuhan, Kinerja: UDP vs TCP, dan overhead enkripsi, Manajemen versi dan pemeliharaan dan Konteks ancaman nasional.⁵

Berdasarkan persoalan yang telah diuraikan sebelumnya, penelitian tentang “Implementasi dan Analisis Jaringan VPN Menggunakan OpenVPN pada Jaringan Lokal” menjadi sangat krusial. Penelitian ini penting dilakukan karena dapat memberikan panduan praktis bagi organisasi dalam merancang arsitektur VPN yang sesuai dengan kebutuhan, baik untuk skema remote access maupun site-to-site. Selain itu, penelitian ini juga membantu organisasi dalam menentukan topologi jaringan yang tepat, seperti penggunaan metode routing atau bridging, serta menetapkan kebijakan akses yang aman. Penelitian ini juga memiliki urgensi dalam memvalidasi kinerja OpenVPN pada skenario nyata di jaringan lokal. Hal ini dilakukan dengan membandingkan parameter penting seperti throughput, latensi, packet loss, dan penggunaan CPU, baik ketika menggunakan protokol UDP maupun TCP. Analisis juga mencakup perbandingan variasi algoritma kriptografi seperti AES-GCM dan ChaCha20-Poly1305, serta pengaruh ukuran MTU dan TUN-MSS terhadap stabilitas koneksi.

Selain kinerja, penelitian ini juga berfokus pada aspek keamanan melalui penerapan hardening konfigurasi sesuai dengan praktik terbaru. Hal ini meliputi penggunaan minimal TLS 1.2, penerapan Perfect Forward Secrecy (ECDHE), sertifikat yang kuat, pemblokiran cipher lama yang tidak lagi direkomendasikan,

⁵ Hidayat, M. (2022). Analisis Kinerja VPN Menggunakan OpenVPN pada Jaringan Lokal. Jurnal Teknologi Informasi, 6(1), 15–22.

serta penguatan sisi server dengan aturan firewall seperti iptables/nftables. Lebih jauh lagi, penelitian ini menekankan pentingnya pengaturan tambahan seperti client-specific overrides, client-config-dir, serta penerapan split-tunneling yang terkontrol. Tidak hanya itu, penelitian ini juga mendorong kepatuhan dan kesiapan audit dalam implementasi jaringan VPN. Hal ini dapat dicapai melalui dokumentasi yang rapi mengenai arsitektur jaringan, parameter kriptografi, serta kebijakan pembaruan sistem. Proses ini diperkuat dengan penerapan sistem logging yang komprehensif dan pemantauan yang berkesinambungan, seperti pengumpulan log secara terpusat, deteksi anomali trafik, maupun peringatan dini terhadap koneksi yang gagal.

Dengan demikian, penelitian ini diharapkan mampu menghasilkan bukti empiris sekaligus panduan konfigurasi yang dapat langsung direplikasi pada jaringan lokal organisasi. Hal ini tentu akan memberikan kontribusi nyata dalam upaya peningkatan keamanan jaringan, efisiensi operasional, serta ketahanan terhadap ancaman siber yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dibahas, maka rumusan masalah dalam penelitian ini ialah sebagai berikut:

1. Bagaimana cara mengimplementasikan OpenVPN pada jaringan lokal?
2. Bagaimana kinerja jaringan sebelum dan sesudah menggunakan OpenVPN?
3. Apa saja kelebihan dan kekurangan penggunaan OpenVPN di jaringan lokal?

1.3 Batasan Masalah

Penelitian ini dibatasi pada tiga aspek utama agar pembahasan lebih terarah dan fokus yaitu:

1. Penelitian hanya membahas bagaimana cara mengimplementasikan OpenVPN pada jaringan lokal, sehingga ruang lingkupnya terbatas pada proses instalasi, konfigurasi server dan klien, serta pengaturan dasar keamanan. Penelitian tidak membahas implementasi VPN lain seperti IPsec atau WireGuard, dan juga tidak membahas integrasi dengan layanan cloud atau sistem identitas tingkat lanjut.
2. Penelitian difokuskan pada analisis kinerja jaringan sebelum dan sesudah menggunakan OpenVPN. Parameter yang diukur mencakup throughput, latensi, dan stabilitas koneksi dalam konteks jaringan lokal. Analisis tidak mencakup uji coba pada skala jaringan luas (wide area network) atau lingkungan produksi berskala besar yang memiliki kompleksitas tinggi.
3. Penelitian hanya menilai kelebihan dan kekurangan penggunaan OpenVPN di jaringan lokal berdasarkan hasil implementasi dan pengujian yang dilakukan. Aspek yang ditinjau meliputi kemudahan penggunaan, tingkat keamanan, dan performa dasar. Penelitian tidak membahas perbandingan mendalam dengan perangkat lunak VPN komersial lainnya maupun evaluasi terkait faktor ekonomi, seperti biaya lisensi perangkat lunak atau perangkat keras tambahan.

Dengan adanya batasan tersebut, penelitian ini diharapkan tetap fokus, terarah, dan dapat memberikan hasil yang jelas serta bermanfaat dalam konteks implementasi OpenVPN di jaringan lokal.

1.4 Tujuan Penelitian

Melihat rumusan masalah dan batasan masalah, maka tujuan dalam penelitian ini ialah sebagai berikut:

1. Menerapkan OpenVPN pada jaringan lokal.
2. Mengukur dan menganalisis performa jaringan (latency, throughput, kecepatan transfer data).
3. Mengevaluasi dampak keamanan dan performa setelah penerapan OpenVPN.

1.5 Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan khususnya di bidang jaringan komputer dan keamanan informasi. Hasil penelitian mengenai implementasi dan analisis OpenVPN pada jaringan lokal dapat menambah referensi akademik mengenai penerapan teknologi VPN berbasis open source. Selain itu, penelitian ini juga dapat menjadi dasar teoritis bagi penelitian selanjutnya yang ingin mengkaji lebih dalam mengenai kinerja, keamanan, maupun perbandingan antarprotokol VPN. Dengan adanya kajian ini, diharapkan literatur mengenai jaringan aman berbasis VPN semakin kaya dan dapat digunakan sebagai rujukan dalam pengembangan konsep maupun pembelajaran di bidang teknologi informasi.

2. Manfaat Praktis

Secara praktis, penelitian ini memberikan manfaat bagi organisasi, instansi pendidikan, maupun individu yang ingin menerapkan solusi jaringan aman menggunakan OpenVPN. Hasil penelitian dapat menjadi panduan implementasi yang jelas mulai dari tahap instalasi, konfigurasi, hingga pengujian kinerja sehingga memudahkan dalam penerapan nyata di jaringan lokal. Selain itu, penelitian ini dapat membantu administrator jaringan dalam memahami kelebihan dan kekurangan OpenVPN, sehingga mereka dapat mengambil keputusan yang tepat dalam pemilihan teknologi VPN sesuai kebutuhan. Bagi praktisi, penelitian ini juga memberikan gambaran nyata mengenai perbedaan kinerja jaringan sebelum dan sesudah penggunaan OpenVPN, sehingga dapat dijadikan dasar dalam meningkatkan efisiensi sekaligus memperkuat aspek keamanan jaringan.

1.6 Sistematika Penulisan

Bab I Pendahuluan

Bab ini berisi uraian mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Bagian ini memberikan gambaran umum mengenai alasan dilaksanakannya penelitian, arah penelitian, serta manfaat yang diharapkan.

Bab II Landasan Teori

Bab ini membahas teori-teori yang mendukung penelitian, termasuk konsep dasar jaringan komputer, teknologi Virtual Private Network (VPN), prinsip kerja

OpenVPN, standar keamanan jaringan, serta penelitian-penelitian terdahulu yang relevan. Selain itu, bab ini juga menguraikan kerangka berpikir yang menjadi landasan dalam menganalisis hasil penelitian.

Bab III Analisis dan Perencanaan Sistem

Bab ini menjelaskan metode yang digunakan dalam penelitian, meliputi jenis penelitian, lokasi dan waktu penelitian, alat dan bahan yang digunakan, tahapan implementasi OpenVPN, serta metode pengujian kinerja jaringan. Bagian ini juga memaparkan teknik pengumpulan data, parameter yang diukur (misalnya throughput, latensi, packet loss), serta metode analisis yang digunakan.

Bab IV Implementasi dan Pembahasan

Bab ini menyajikan hasil implementasi OpenVPN pada jaringan lokal, termasuk tahapan instalasi, konfigurasi server dan klien, serta penerapan hardening keamanan. Selanjutnya, ditampilkan hasil pengujian kinerja jaringan sebelum dan sesudah menggunakan OpenVPN. Data hasil pengujian kemudian dianalisis dan dibahas secara mendalam untuk mengetahui kelebihan dan kekurangan penggunaan OpenVPN.

Bab V Penutup

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya maupun untuk penerapan nyata di lapangan. Kesimpulan akan menjawab rumusan masalah, sedangkan saran diberikan untuk pengembangan lebih lanjut agar hasil penelitian dapat lebih optimal dan bermanfaat.

Daftar Pustaka

Berisi sumber-sumber referensi yang digunakan dalam penelitian ini, baik berupa buku, jurnal, artikel ilmiah, maupun sumber daring yang relevan dan terbaru.

Lampiran

Memuat data pendukung penelitian, se

