

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan layanan berbasis internet dan teknologi jaringan terutama sejak era kerja dan pembelajaran jarak jauh menjadikan *Virtual Private Network (VPN)* sebagai solusi penting untuk menjamin keterhubungan antarjaringan melalui internet publik. *VPN* memungkinkan perangkat di luar jaringan internal mengakses sumber daya internal secara aman dengan membuat terowongan terenkripsi antara klien dan server, sehingga data sensitif tidak mudah disadap saat melintasi jaringan publik. Implementasi *OpenVPN*, *L2TP/IPsec*, dan protokol *VPN* lain banyak diteliti pada konteks institusi dan perusahaan di Indonesia sebagai respons terhadap kebutuhan *Work From Home (WFH)* dan akses jarak jauh (Febriyanto & Sobari, 2024).

Secara teknis, *VPN* meningkatkan kerahasiaan dan integritas data lewat enkripsi dan autentikasi *end-to-end*, mengurangi risiko kebocoran informasi saat penggunaan jaringan publik. Namun, penggunaan *VPN* juga membawa *trade-off*: enkripsi dan routing tambahan dapat menimbulkan overhead yang berdampak pada *latency*, *throughput*, dan pengalaman pengguna, masalah yang penting ketika layanan yang diakses memerlukan *bandwidth* tinggi seperti media pembelajaran atau konferensi video. Oleh karena itu, berbagai penelitian di Indonesia berfokus pada evaluasi performa, perbandingan protokol, dan pengoptimalan konfigurasi *VPN* guna menemukan titik keseimbangan yang ideal antara aspek keamanan dan performa jaringan (Pribadi Fitriani *et al.*, 2025).

Sementara itu, pada lingkungan institusi pendidikan seperti sekolah dan kampus, tantangan implementasi *VPN* menjadi semakin kompleks karena melibatkan keterbatasan sumber daya perangkat keras, kapabilitas teknis pengelola jaringan, dan kebijakan internal terkait manajemen akses. Pemilihan jenis *VPN* yang tepat baik *Remote Access* untuk koneksi individu maupun *site-to-site* untuk menghubungkan antar jaringan harus mempertimbangkan infrastruktur yang tersedia serta kompatibilitas dengan perangkat dan sistem yang sudah digunakan. Selain itu, proses konfigurasi *Network Address Translation (NAT)*, pengaturan *firewall*, ketersediaan alamat IP publik, hingga pemanfaatan layanan *Dynamic DNS* sering kali menjadi hambatan teknis yang memerlukan solusi kreatif dan efisien. Beberapa studi kasus di Indonesia menunjukkan bahwa keberhasilan penerapan *VPN* di sektor pendidikan sangat bergantung pada perencanaan arsitektur jaringan yang matang, uji performa yang komprehensif, serta dokumentasi prosedur operasional yang jelas bagi administrator jaringan (Masroni *et al.*, 2021).

Salah satu *VPN* yang efektif dan efisien adalah penerapan *OpenVPN*, sebuah perangkat lunak open-source yang digunakan untuk membangun koneksi jaringan pribadi secara aman melalui internet. *OpenVPN* menawarkan berbagai keunggulan, seperti sifatnya yang *open-source*, *cross-platform*, serta mendukung enkripsi tingkat tinggi. Dengan protokol *SSL/TLS*, *OpenVPN* mampu memberikan keamanan data yang kuat sekaligus stabilitas koneksi. Keunggulan lainnya adalah sifatnya yang fleksibel dan dapat disesuaikan dengan kebutuhan berbagai jenis jaringan. Karena tidak memerlukan biaya lisensi, *OpenVPN* sangat cocok digunakan di lingkungan sekolah yang memiliki keterbatasan anggaran. Selain itu, *OpenVPN* juga mendapat dukungan komunitas global yang luas, sehingga

memudahkan proses konfigurasi dan pemecahan masalah teknis (Affandi, 2022). *OpenVPN* menonjol karena sifatnya yang *open-source*, mendukung berbagai metode enkripsi yang kuat seperti (*AES-256*), dan fleksibilitas konfigurasinya. Oleh karena itu, *OpenVPN* menjadi pilihan populer untuk organisasi yang mengutamakan keamanan serta performa dalam konektivitas jarak jauh. Namun, meskipun teknologi *VPN* seperti *OpenVPN* menjanjikan peningkatan keamanan, implementasinya juga menimbulkan tantangan. Menurut Wulandari, (2024) terdapat penurunan throughput dan peningkatan latency dibandingkan dengan koneksi tanpa *VPN*, hal ini disebabkan oleh proses enkripsi-dekripsi data yang memerlukan waktu pemrosesan lebih besar sekaligus memberikan koneksi yang relatif stabil, bahkan pada jaringan dengan bandwidth terbatas.

Menurut Nugroho *et al.*, (2025) salah satu tantangan teknis yang sering dihadapi adalah penggunaan IP publik dinamis dari penyedia layanan internet (*ISP*). IP dinamis bersifat berubah-ubah secara berkala, sehingga menyulitkan administrator jaringan untuk melakukan *Remote Access* atau pemantauan perangkat dari luar jaringan sekolah secara konsisten. Ketidadaan IP statis menyebabkan kendala dalam menjaga konektivitas yang stabil dan aman untuk pengelolaan sistem jaringan dari jarak jauh. Untuk mengatasi permasalahan ini, *Free Dynamic DNS (FreeDDNS)* menjadi solusi yang efektif. *FreeDDNS* memungkinkan pemetaan antara nama domain tetap dengan IP dinamis, sehingga perangkat seperti router MikroTik tetap dapat diakses meskipun alamat IP-nya berubah. Penggunaan *FreeDDNS* sangat relevan untuk lingkungan sekolah karena mudah dikonfigurasi dan mendukung integrasi dengan sistem keamanan jaringan seperti *OpenVPN*.

Mikrotik RouterOS menyediakan berbagai fitur penting yang mendukung kebutuhan jaringan sekolah, seperti *Virtual Private Network (VPN)*, *Dynamic DNS (DDNS)*, *firewall*, *Quality of Service (QoS)*, hotspot, dan manajemen bandwidth. Keunggulan ini menjadikan Mikrotik mampu menangani kebutuhan infrastruktur jaringan skala menengah dengan optimal, sekaligus memberikan keamanan jaringan yang lebih baik. Sebagai contoh, fitur *firewall* pada Mikrotik dapat dikonfigurasi secara kompleks untuk memblokir akses tidak sah, mengatur bandwidth, dan melakukan autentikasi pengguna. Ini sangat bermanfaat untuk melindungi perangkat dan data di laboratorium komputer sekolah (Pratomo, 2023). Selain itu, sistem operasi Mikrotik RouterOS menawarkan fleksibilitas konfigurasi yang tinggi, baik untuk keperluan jaringan lokal maupun akses jarak jauh (remote access). Hal ini menjadi solusi penting bagi sekolah yang memiliki keterbatasan sumber daya namun membutuhkan keamanan dan kestabilan jaringan untuk mendukung proses pembelajaran digital (Taufiqurrochman *et al.*, 2023).

Dengan karakteristik tersebut, Mikrotik sangat sesuai digunakan untuk implementasi jaringan berskala menengah, seperti di sekolah-sekolah kejuruan. penerapan manajemen jaringan berbasis *QoS* juga dilakukan untuk menjamin kualitas layanan yang digunakan oleh siswa dan guru. Teknologi ini digunakan untuk mengatasi permasalahan seperti perebutan bandwidth, keterbatasan kecepatan akses, serta rendahnya prioritas terhadap layanan penting seperti *HTTP*, *FTP*, dan *SMTP*. Mikrotik menjadi komponen penting dalam arsitektur jaringan sekolah, berperan sebagai router utama dalam mengelola lalu lintas data secara efisien (Tahir *et al.*, 2022).

Penelitian yang dilakukan oleh Riyanto *et al.*, (2025) bertujuan untuk menyelesaikan permasalahan keamanan jaringan dan akses jarak jauh di lingkungan akademis, khususnya di Universitas PGRI Silampari. Sistem jaringan sebelumnya dinilai kurang optimal dalam memberikan perlindungan terhadap data dan tidak mampu menyediakan akses yang aman bagi pengguna luar kampus, seperti staf dan mahasiswa. penelitian ini merancang dan mengimplementasikan sistem *VPN* berbasis MikroTik guna meningkatkan keamanan serta stabilitas koneksi jaringan. Hasil penelitian menunjukkan bahwa penerapan *VPN* berbasis MikroTik secara signifikan meningkatkan kualitas dan keamanan akses jaringan kampus. Sistem yang dikembangkan mampu mengurangi risiko serangan siber hingga 50% dan meningkatkan kecepatan akses jaringan sebesar 30%. Selain itu, pengguna dapat mengakses jaringan kampus secara aman dan efisien dari lokasi eksternal. Dengan demikian, penelitian ini mendukung pengembangan sistem jaringan yang aman dan berkelanjutan di lingkungan pendidikan tinggi, sekaligus dapat dijadikan acuan bagi sekolah atau institusi pendidikan lain yang menghadapi masalah serupa dalam keamanan akses jarak jauh.

Penelitian terdahulu yang dilakukan Hayati *et al.*, (2023) menunjukkan bahwa penerapan *Virtual Private Network (VPN)* berbasis Mikrotik mampu menjadi solusi efektif dalam menyediakan konektivitas jarak jauh yang aman dan efisien bagi guru maupun teknisi sekolah. Melalui implementasi sistem *remote access*, pengguna dari luar sekolah dapat mengakses jaringan internal tanpa harus hadir secara fisik, sehingga mendukung efisiensi kerja dan fleksibilitas operasional. Hasil pengujian membuktikan bahwa koneksi *VPN* berjalan dengan baik, meskipun terdapat variasi latensi pada rentang 276 ms hingga 607 ms, namun tetap berada pada kategori

koneksi stabil dan dapat digunakan untuk kebutuhan manajemen jaringan maupun pertukaran data. Temuan ini memperkuat urgensi bahwa sekolah-sekolah yang belum menerapkan sistem akses jarak jauh sangat membutuhkan *VPN* sebagai sarana peningkatan keamanan, stabilitas, dan efektivitas dalam pengelolaan jaringan.

Penelitian relevan selanjutnya dilakukan oleh Nugroho *et al.*, (2025) bertujuan untuk menambahkan fitur *Remote Access* menggunakan layanan *FreeDDNS* agar pengelolaan jaringan dapat dilakukan dari luar sekolah. Hasil penelitian menunjukkan bahwa setelah alamat *MAC* perangkat didaftarkan, pengguna dapat terhubung secara otomatis tanpa harus login ulang, bahkan ketika berpindah antar *access point*. Hal ini terbukti meningkatkan kenyamanan, efisiensi waktu, serta keamanan jaringan sekolah. Selain itu, penerapan *Remote Access* dengan *FreeDDNS* berhasil memungkinkan administrator mengakses Mikrotik dari luar jaringan sekolah, sehingga mendukung manajemen jaringan jarak jauh. Dengan demikian penelitian ini memberikan kontribusi nyata terhadap peningkatan keamanan dan fleksibilitas pengelolaan jaringan di lingkungan pendidikan.

SMKN 1 Kwanyar merupakan salah satu sekolah menengah kejuruan yang memiliki berbagai program keahlian berbasis teknologi dan informatika. Seiring dengan berkembangnya sistem pendidikan yang semakin terdigitalisasi, kebutuhan terhadap akses jaringan yang aman, handal, dan fleksibel menjadi semakin mendesak. Aktivitas penting seperti pengelolaan server sekolah, pemantauan jaringan laboratorium, hingga akses terhadap sistem pembelajaran berbasis intranet menuntut adanya koneksi yang dapat diakses dari luar lingkungan sekolah secara konsisten dan terlindungi. Berdasarkan hasil observasi dan wawancara pada tanggal

27 November 2025 dengan Bapak Ainul Yakin, S.Kom selaku guru sekaligus Ketua *MGMP* Teknik Komputer dan Jaringan, diketahui bahwa kondisi infrastruktur jaringan komputer di sekolah sudah tergolong cukup baik dan telah tersedia akses internet. Perangkat utama yang digunakan meliputi *modem* yang disalurkan ke *switch* dan *router* sebagai pendukung jaringan internal. Meskipun demikian, teknisi maupun guru masih mengalami kendala ketika harus mengakses jaringan dari luar sekolah. Beberapa kali terjadi situasi dimana guru atau teknisi ditugaskan menangani masalah jaringan dari luar, tetapi tidak dapat terhubung karena belum adanya infrastruktur maupun mekanisme resmi untuk *remote access*. Kendala utama ini diperparah dengan keterbatasan SDM dan belum tersedianya standar operasional prosedur (*SOP*) yang menjamin keamanan ketika mengakses jaringan dari luar.

Selain itu, meskipun SMKN 1 Kwanyar telah memiliki sejumlah perangkat jaringan yang terletak pada Laboratorium TKJ, sekolah saat ini menggunakan IP dinamis dari *ISP AlfaNet* sehingga alamat IP sering berubah dan menyulitkan proses akses jarak jauh. Teknologi *VPN* sebenarnya pernah dicoba, namun belum diterapkan secara resmi karena masih adanya kekhawatiran terhadap keamanan data sekolah. Pihak sekolah juga belum pernah mempertimbangkan penerapan *VPN* sebagai solusi keamanan dan akses jarak jauh.

Berdasarkan hasil observasi, wawancara dengan pihak terkait, serta telaah terhadap penelitian sebelumnya, peneliti menyimpulkan bahwa solusi yang paling tepat adalah menerapkan *VPN* menggunakan *OpenVPN* yang dipadukan dengan layanan *FreeDDNS*. Layanan *FreeDDNS* mampu menyediakan domain yang bersifat tetap meskipun IP publik berubah-ubah, sehingga lebih andal untuk

kebutuhan penggunaan jangka panjang. Di sisi lain, *OpenVPN* memberikan jalur komunikasi terenkripsi dari ujung ke ujung, sehingga keamanan data selama proses akses jarak jauh tetap terjaga. Melalui kombinasi keduanya, kegiatan pengelolaan jaringan sekolah dapat dilakukan dengan lebih aman, stabil, dan efisien. Atas dasar pertimbangan tersebut, penelitian ini mengusung judul “Implementasi *VPN Remote Access* Berbasis *OpenVPN & FreeDDNS* untuk Meningkatkan Keamanan Akses Jaringan MikroTik di SMKN 1 Kwanyar.” sebagai bentuk kontribusi nyata dalam meningkatkan keamanan, fleksibilitas, dan efektivitas pengelolaan jaringan sekolah.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan, peneliti menentukan rumusan masalah seperti berikut :

1. Bagaimana rancangan dan implementasi *VPN Remote Access* berbasis *OpenVPN* dan *FreeDDNS* dengan Mikrotik di SMKN 1 Kwanyar?
2. Bagaimana hasil pengujian koneksi *VPN Remote Access* berbasis *OpenVPN* dan *FreeDDNS* dengan parameter *Quality of Service (QoS)*?

1.3 Tujuan Penelitian Pengembangan

1. Merancang dan mengimplementasikan sistem *VPN Remote Access* berbasis *OpenVPN* yang terintegrasi dengan layanan *FreeDDNS* pada perangkat Mikrotik, sebagai solusi akses jaringan internal secara aman dan fleksibel di SMKN 1 Kwanyar.

2. Menguji dan menganalisis kinerja koneksi *VPN* yang dibangun berdasarkan parameter *Quality of Service (QoS)* seperti *throughput*, *jitter*, *delay*, dan *packet loss* guna memastikan kualitas layanan jaringan yang memadai untuk kebutuhan *remote access*.

1.4 Spesifikasi Produk Yang Diharapkan

Peneliti mengharapkan spesifikasi produk dalam penelitian ini mencakup aspek-aspek berikut :

1. *Router Mikrotik* merupakan perangkat jaringan yang menggunakan sistem operasi RouterOS, dikembangkan oleh perusahaan *MikroTik* asal *Latvia*. Perangkat ini dirancang untuk mengelola lalu lintas data dalam jaringan komputer dan menawarkan berbagai fitur jaringan yang canggih namun tetap terjangkau, sehingga sangat populer di kalangan teknisi jaringan, termasuk di lingkungan pendidikan.
2. Integrasi *OpenVPN* system dapat membangun dan mengelola koneksi *Virtual Private Network (VPN)*, dengan menggunakan *OpenVPN* yang bersifat *open-source* serta dukungan protokol enkripsi TLS untuk menjamin keamanan lalu lintas data.
3. *FreeDDNS* adalah layanan *Dynamic DNS* yang memungkinkan pemetaan IP dinamis dari *ISP* ke nama domain tetap. Ini sangat berguna bagi sekolah yang tidak memiliki IP statis, karena alamat IP publik bisa berubah-ubah. Dengan *FreeDDNS* , pengguna cukup mengakses jaringan sekolah melalui nama domain (misalnya: *smkn1kwanyar.freedns.org*) yang otomatis diperbarui saat IP berubah. Solusi ini cocok untuk digunakan bersama

MikroTik dan *VPN*, karena gratis, mudah dikonfigurasi, dan menjaga akses jarak jauh tetap stabil.

4. *Remote Access* memungkinkan guru, teknisi jaringan, atau administrator sekolah untuk mengakses sumber daya jaringan lokal sekolah dari luar lingkungan sekolah secara aman dan konsisten.

1.5 Batasan Penelitian Pengembangan

Penelitian ini memiliki beberapa batasan yang ditetapkan untuk memperjelas ruang lingkup kajian, yaitu sebagai berikut:

1. Merancang serta mengimplementasikan *Virtual Private Network (VPN)* dalam penelitian ini dilakukan secara terbatas di lingkungan laboratorium komputer SMKN 1 Kwanyar sebagai lokasi uji coba utama.
2. Perangkat yang digunakan *MikroTik RouterOS*.
3. *Virtual Private Network* yang dirancang menggunakan protokol *OpenVPN* dan terintegrasi *FreeDDNS*
4. Konfigurasi *MikroTik* menggunakan aplikasi *WinBox* pada perangkat Laptop/PC.
5. Untuk IP Publik menggunakan layanan pihak ketiga yaitu *FreeDDNS*
6. Penelitian yang dilakukan hanya perancangan *Virtual Private Network OpenVPN* dan *FreeDDNS* untuk pemetaan antara nama domain tetap dengan IP Dinamis.
7. Pengujian yang dilakukan menguji koneksi *Virtual Private Network, Remote Access MikroTik*, melakukan ping pada perangkat yang terhubung

dijaringan lokal, melihat dari parameter *Throughput*, *Jitter*, *Delay*, dan *Packet Loss*.

1.6 Pentingnya Penelitian Pengembangan

Penelitian ini diharapkan dapat memberikan beberapa manfaat, baik secara teoritis maupun praktis, yang dijelaskan sebagai berikut:

1. Manfaat Teoritis

Penelitian ini berkontribusi pada pengembangan pengetahuan di bidang jaringan komputer, khususnya mengenai integrasi antara *OpenVPN*, *FreeDDNS*, dan perangkat Mikrotik dalam membangun sistem *Remote Access* yang aman. Hasil dari penelitian ini dapat menjadi referensi akademik maupun dasar pengembangan model sistem keamanan jaringan bagi institusi pendidikan lainnya yang menghadapi keterbatasan IP publik dan infrastruktur terbatas.

2. Secara Praktis

Penelitian ini memberikan solusi langsung yang dapat diterapkan untuk meningkatkan efisiensi dan keamanan pengelolaan jaringan di SMKN 1 Kwanyar. Dengan adanya sistem *VPN* yang terintegrasi, guru dan teknisi dapat mengakses jaringan internal sekolah dari luar secara aman dan stabil. Selain itu, sistem ini dapat dijadikan prototipe implementasi serupa di sekolah lain dengan kondisi infrastruktur jaringan yang sebanding.

1.7 Definisi Istilah

1. *VPN (Virtual Private Network)* adalah suatu metode untuk membuat koneksi aman dan terenkripsi melalui jaringan publik seperti internet, sehingga pengguna dapat mengakses jaringan lokal dari jarak jauh seolah-olah berada dalam satu jaringan yang sama.
2. *OpenVPN* merupakan protokol *open-source* untuk membangun jaringan *VPN* yang aman dan fleksibel. *OpenVPN* menggunakan protokol *SSL/TLS* dan mendukung berbagai sistem operasi, serta dapat dikonfigurasi pada perangkat *MikroTik*.
3. *FreeDDNS (Free Dynamic Domain Name System)* Layanan *DNS* dinamis gratis yang memungkinkan pengguna memetakan IP dinamis ke nama domain tetap, sehingga tetap dapat mengakses jaringan meskipun alamat IP berubah secara berkala.
4. *MikroTik RouterOS* adalah Sistem operasi berbasis *Linux* yang dikembangkan oleh perusahaan *Mikrotik*, digunakan untuk mengelola dan mengatur jaringan komputer, termasuk konfigurasi *VPN*, *firewall*, dan *QoS*.
5. *Remote Access* merupakan akses ke jaringan atau sistem komputer dari lokasi yang berbeda atau luar jaringan lokal, biasanya menggunakan koneksi *VPN* yang aman.