

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sedang mengalami kemajuan yang pesat, terutama di bidang teknologi informasi yang dimulai dari perangkat komputer hingga aplikasi yang membantu manusia dalam berbagai aktivitasnya. Sistem komputer memberikan kenyamanan dalam berurusan dengan masalah teknologi informasi, dan internet menjadi dampak besar yang mempengaruhi berbagai aspek kehidupan manusia. Koneksi internet dan penggunaan online yang semakin tinggi menuntut perangkat dan teknologi informasi untuk terus berkembang dan menjadi semakin canggih dalam memberikan hasil maksimal, efisiensi, dan peningkatan keamanan. Di masa depan, perkembangan teknologi informasi diperkirakan akan terus berlanjut dengan inovasi terbaru untuk membantu manusia menghadapi tantangan dan masalah di era digital (Sumarna & Maulana, 2021).

Teknologi informasi membawa era baru dalam dunia informasi modern dan telah berkembang pesat selama beberapa tahun terakhir. Berbagai teknologi informasi seperti komputer, internet, dan aplikasi berbasis teknologi telah membantu mengubah cara kita belajar dan memberikan aksesibilitas yang lebih besar ke informasi. Dengan teknologi informasi, siswa dapat memperoleh akses ke bahan-bahan pelajaran online, mengikuti kelas virtual, dan berkomunikasi dengan rekan sekelas dan guru dari jarak jauh. Teknologi informasi juga memungkinkan proses belajar mengajar yang lebih interaktif dan menarik, serta memberikan kesempatan bagi siswa dan guru untuk meningkatkan efisiensi dan produktivitas dalam proses pendidikan. Oleh karena itu, peranan teknologi informasi pada aktivitas manusia, termasuk dalam bidang pendidikan, sangat penting dan membawa dampak positif bagi masyarakat secara keseluruhan (Kadir & Triwahyuni, 2014).

Teknologi komputer sudah menjadi bagian dari berbagai bidang, termasuk pendidikan. Sebagian besar sekolah telah menggunakan komputer untuk

mempercepat proses kerja administrasi dan akademik. Selain itu, teknologi komputer juga dimanfaatkan untuk mendukung proses pembelajaran. Komputer dijadikan sebagai media untuk mengajar sehingga konsep keilmuan menjadi lebih menarik dan mudah diterima oleh siswa. Bahkan, kini banyak sekolah yang memiliki jaringan komputer yang mengintegrasikan jaringan lokal ke jaringan intranet dan internet (Kadir & Triwahyuni, 2014). Ada juga sekolah yang memanfaatkan teknologi telepon seluler untuk proses pembelajaran dan layanan sekolah, seperti di SMK NU 1 Kedungpring Lamongan.

Keamanan jaringan dalam jaringan komputer sangatlah penting untuk dilakukan, terutama untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Seorang administrator jaringan bertanggung jawab mengontrol tugas keamanan jaringan tersebut. Tujuan utama keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan yang berupa ancaman fisik maupun logika yang dapat mengganggu aktivitas dalam jaringan komputer baik langsung maupun tidak langsung (Kadir & Triwahyuni, 2014). Hal ini juga berlaku di SMK NU 1 Kedungpring, di mana menjaga keamanan jaringan di sekolah menjadi prioritas dalam rangka menghindari potensi ancaman keamanan dan menjaga ketersediaan dan integritas jaringan komputer.

Implementasi jaringan VPN dengan protocol *OpenVPN* di SMK NU 1 Kedungpring merupakan solusi untuk memastikan keamanan dan privasi data yang dikirimkan melalui jaringan (Langobelen et al., 2019). Meski begitu, beberapa protokol VPN, termasuk *OpenVPN*, memiliki celah keamanan yang dapat dimanfaatkan oleh peretas. Oleh karena itu, implementasi keamanan jaringan VPN harus dilakukan dengan konfigurasi yang benar dan tepat. Sebaliknya, jaringan VPN yang kurang terlindungi akan mudah ditembus oleh peretas, terutama pada jaringan yang kompleks. Maka, konfigurasi yang tepat dan benar sangat penting untuk memastikan keamanan jaringan VPN di SMK NU 1 Kedungpring.

*Virtual Private Network* (VPN) merupakan suatu teknologi yang digunakan untuk membangun jaringan yang aman dan terpecah pada jaringan

publik, seperti Internet. VPN menggunakan protokol enkripsi untuk mengamankan data yang dikirim dan diterima melalui jaringan publik, sehingga data tersebut tidak dapat diakses oleh orang yang tidak berwenang.

*Virtual Private Network (VPN)* menjadi salah satu solusi keamanan teknologi komunikasi pada jaringan internet. Jenis komunikasi ini memungkinkan data yang kita kirim melalui jalur koneksi terenkripsi di jaringan publik namun sifatnya private. Ada beberapa protokol VPN yang bisa digunakan, dari teknologi open source sampai yang berbayar. Namun, setiap protokol VPN yang berbeda tentunya dapat mempengaruhi kinerja jaringan throughput meskipun ukuran *bandwidth* pada server dan client sama. Salah satu protokol yang dapat menambahkan keamanan jaringan VPN adalah dengan menggunakan teknologi *OpenVPN*. Dalam teknologi *OpenVPN*, data yang dikirim melalui jaringan terenkripsi menggunakan kunci akses simetris dan asimetris sehingga lebih aman dan tidak mudah diakses oleh pihak yang tidak berwenang (Sidik et al., 2021). *MikroTik RouterOS* adalah sistem operasi untuk perangkat jaringan yang menyediakan fitur VPN dengan protokol *OpenVPN* (Purba & Simanjuntak, 2021).

Dalam era digital saat ini, jaringan komputer telah menjadi bagian penting dari kehidupan sehari-hari. Peningkatan penggunaan internet dan akses jaringan dari berbagai perangkat telah mendorong perusahaan atau institusi untuk mengimplementasikan jaringan yang aman dan terlindungi (Amarudin, 2018). Salah satu cara untuk memastikan keamanan jaringan adalah dengan menggunakan jaringan VPN (*Virtual Private Network*). SMK NU 1 Kedungpring sebagai salah satu lembaga pendidikan juga menghadapi tantangan untuk menyediakan jaringan yang aman bagi siswa dan staf. Oleh karena itu, implementasi jaringan VPN dengan protokol *OPENVPN* menggunakan *MikroTik RouterOS* di SMK NU 1 Kedungpring merupakan solusi untuk memastikan keamanan dan privasi data yang dikirimkan melalui jaringan.

Permasalahan yang ditemukan peneliti serta Konfigurasi jaringan VPN yang kompleks pada SMK NU 1 Kedungpring mungkin menjadi sebuah permasalahan yang harus diperhatikan. Sebagai jaringan yang digunakan oleh banyak pengguna, pengaturan konfigurasi yang salah dapat berakibat pada

jaringan yang tidak stabil dan rentan terhadap serangan. Hal ini membutuhkan ketelitian dan keahlian dalam melakukan pengaturan konfigurasi yang tepat dan efektif. Konfigurasi yang tidak tepat pada jaringan VPN dapat membuat jaringan menjadi mudah ditembus oleh peretas dan data yang terkirim melalui jaringan dapat terbaca oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan pengaturan konfigurasi yang benar dan tepat untuk memastikan keamanan jaringan VPN di SMK NU 1 Kedungpring. Dalam membangun dan merancang *virtual private network* dengan permasalahan yang disampaikan, maka penulis mengangkat judul skripsi “**Analisis Dan Implementasi Keamanan Jaringan VPN Menggunakan Protokol *OpenVPN* Dengan *MikroTik RouterOS* (Studi Kasus di SMK NU 1 Kedungpring)**”.

## 1.2 Rumusan Masalah

Dari uraian Latar Belakang diatas, penulis dapat menyimpulkan beberapa rumusan masalah yaitu :

1. Bagaimana Implementasi dan Konfigurasi VPN menggunakan protokol *OpenVPN* dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring?
2. Bagaimana Mengembangkan Keamanan Jaringan VPN Menggunakan Protokol *OpenVPN* Dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring?
3. Bagaimana Menguji Kelayakan Keamanan Jaringan VPN Menggunakan Protokol *OpenVPN* Dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring?

## 1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan dari penelitian ini adalah :

1. Implementasi dan Konfigurasi VPN menggunakan protokol *OpenVPN* dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring.
2. Mengembangkan Keamanan Jaringan VPN Menggunakan Protokol *OpenVPN* Dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring.

3. Menguji Kelayakan Keamanan Jaringan VPN Menggunakan Protokol *OpenVPN* Dengan *MikroTik RouterOS* di SMK NU 1 Kedungpring.

#### 1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka di buat batasan masalah yaitu :

1. Perangkat yang digunakan *MikroTik RB941-2nD* dan *Tp Link Wi-Fi Router*.
2. Lokasi penelitian dalam perancangan Keamanan Jaringan VPN dilakukan di kantor SMK NU 1 Kedungpring.
3. Konfigurasi *MikroTik* menggunakan aplikasi WinBox pada perangkat PC.
4. *Virtual Private Network* yang dirancang menggunakan protokol Layer 2 *Tunneling Protocol* dan *IPSec (OpenVPN)*.
5. Untuk IP Publik menggunakan jasa layanan ISP Indihome
6. Penelitian yang dilakukan hanya perancangan virtual private network dengan tambahan mengonfigurasi *MikroTik* untuk terhubung ke jaringan internet dan konfigurasi *Tp Link Wi-Fi Router* menjadi akses poin untuk perangkat yang terhubung di jaringan lokal.
7. Pengujian yang dilakukan menguji koneksi *virtual private network*, remote *MikroTik*, melakukan ping pada perangkat yang terhubung di jaringan lokal, remote *Tp Link Wi-Fi Router*, serta pengujian remote desktop untuk pertukaran file.

#### 1.5 Manfaat Penelitian

Berdasarkan hasil penelitian ini diharapkan dapat memberikan kontribusi yang bermanfaat bagi perkembangan ilmu pengetahuan diantaranya sebagai berikut.

1. Memberikan solusi untuk masalah keamanan jaringan VPN di SMK NU 1 Kedungpring.

2. Meningkatkan tingkat keamanan jaringan VPN dengan menggunakan *OpenVPN* dan *MikroTik RouterOS*.
3. Memberikan gambaran bagaimana analisis dan implementasi keamanan jaringan VPN dilakukan pada lingkungan sekolah.
4. Memberikan pemahaman tentang pentingnya keamanan jaringan VPN bagi organisasi dan perusahaan.
5. Memberikan pengetahuan bagaimana menggunakan *MikroTik RouterOS* untuk mengimplementasikan keamanan jaringan VPN.
6. Memberikan dasar teori bagi peneliti lain untuk melakukan penelitian lebih lanjut mengenai keamanan jaringan VPN.
7. Menjadi bahan referensi bagi para praktisi dan pembuat kebijakan dalam bidang teknologi informasi untuk memahami dan membuat solusi keamanan jaringan VPN.

## 1.6 Definisi Istilah

Beberapa definisi istilah yang digunakan dalam penelitian ini sebagai berikut.

1. Analisis  
proses pengkajian dan pemahaman terhadap suatu sistem atau teknologi, dalam hal ini adalah keamanan jaringan VPN menggunakan protokol *OpenVPN* dengan *MikroTik RouterOS*.
2. Implementasi  
proses penerapan dan pengaplikasian suatu solusi atau teknologi, dalam hal ini adalah penerapan keamanan jaringan VPN menggunakan protokol *OpenVPN* dengan *MikroTik RouterOS*.
3. Keamanan Jaringan VPN  
suatu teknologi yang membuat jaringan privasi (*private network*) yang menjaga informasi dan data dari akses yang tidak sah.
4. Protokol *OpenVPN*  
suatu protokol yang digunakan untuk menyediakan koneksi VPN yang aman dan cepat.

### 5. MikroTik RouterOS

suatu sistem operasi router yang menyediakan fitur-fitur seperti routing, *firewall*, dan VPN.

### 6. Internet

Internet adalah singkatan dari jaringan terhubung karena perannya dalam menghubungkan berbagai jaringan komputer di seluruh dunia.

### 7. Sistem

Sebuah sistem merupakan kumpulan elemen yang saling terhubung atau diatur sedemikian rupa sehingga membentuk sebuah entitas yang utuh.

### 8. Firewall

Solusi keamanan jaringan komputer yang efektif adalah dengan mengimplementasikan sistem perlindungan yang dapat menangkal berbagai ancaman, seperti virus, malware, spam, dan jenis serangan lainnya. Dengan adopsi teknologi ini, jaringan dapat terhindar dari potensi serangan yang dapat merusak integritas dan kerahasiaan data. Sistem ini akan menjaga keutuhan infrastruktur IT dari potensi ancaman digital yang beragam, sehingga entitas dapat beroperasi dalam lingkungan daring dengan keyakinan dan keandalan yang lebih tinggi.

### 9. Topologi

Menyatukan dua atau lebih komputer untuk membentuk suatu jaringan merupakan suatu proses yang melibatkan penghubungan perangkat keras dan pengaturan perangkat lunak yang khusus. Tindakan ini memungkinkan komunikasi dan pertukaran data antara komputer-komputer tersebut. Proses mengaitkan komputer satu dengan yang lain biasa dikenal sebagai "penghubungan jaringan". Langkah pertama melibatkan pemilihan metode penghubung fisik, seperti kabel Ethernet atau teknologi nirkabel seperti Wi-Fi. Setelah perangkat keras terhubung, konfigurasi perangkat lunak diperlukan untuk mengatur alamat IP, subnet mask, dan parameter jaringan lainnya. Semua langkah ini harus dilakukan dengan penuh kehati-hatian agar jaringan yang terbentuk dapat

berfungsi secara optimal dan efisien sesuai dengan tujuan yang diinginkan.

10. IP (*Internet Protocol*)

Rangkaian numerik yang berperan sebagai tanda pengenalan peranti yang tersambung dengan internet atau struktur jaringan lainnya..

