BAB I
PENDAHULUAN

1.1. Latar Belakang

Di era digital yang semakin berkembang pesat, teknologi internet telah menjadi bagian yang tidak terpisahkan dari kehidupan manusia. Internet tidak hanya berfungsi sebagai alat komunikasi, tetapi juga sebagai infrastruktur penting yang mendukung berbagai aktivitas, termasuk dalam sektor bisnis, pendidikan, pemerintahan, dan hiburan[1]. Dalam dunia bisnis, internet memungkinkan perusahaan untuk mengelola operasional dengan lebih efisien, mempercepat proses kerja, dan meningkatkan konektivitas antar tim. Namun, di balik manfaatnya, penggunaan internet yang tidak terkendali juga membawa sejumlah tantangan, terutama dalam hal keamanan data dan efisiensi penggunaan sumber daya jaringan[2].

Seiring dengan meningkatnya ancaman digital seperti peretasan, malware, dan kebocoran data, perusahaan harus menerapkan strategi yang efektif untuk melindungi jaringan pengguna[3]. Salah satu solusi utama yang banyak digunakan adalah *firewall*. Secara global, *firewall* berperan sebagai pengaman jaringan yang mengontrol lalu lintas data antara jaringan internal dan eksternal. Dengan teknologi ini, perusahaan dapat memastikan bahwa hanya data yang sah dan aman yang dapat melewati sistem, sementara potensi ancaman dapat dicegah sejak awal[4]. Salah satu jenis *firewall* yang dapat diterapkan adalah *Filtering firewall*.

Filtering Firewall adalah mekanisme penyaringan konten situs web yang sering diterapkan oleh individu, kelompok, atau organisasi untuk membatasi akses ke situs yang tidak diizinkan oleh otoritas atau tidak relevan dengan tujuan bisnis maupun organisasi[5].

Tujuan utama dari *Filtering firewall* adalah menciptakan jaringan yang lebih aman, efisien, dan terkontrol. Sistem ini tidak hanya melindungi jaringan dari ancaman eksternal, tetapi juga meminimalkan risiko

penyalahgunaan akses internet di dalam organisasi. Dengan membatasi akses ke konten yang tidak relevan dan memastikan *Bandwidth* digunakan secara optimal, *Filtering firewall* mendukung peningkatan produktivitas karyawan serta efisiensi operasional perusahaan[6].

Fokus utama dalam mengatasi potensi modifikasi atau kerusakan yang dapat dilakukan oleh penyerang pada router MikroTik adalah dengan meningkatkan tingkat keamanannya. Jaringan MikroTik sangat rentan terhadap berbagai jenis serangan, terutama yang memanfaatkan port-port yang terbuka. Salah satu solusi efektif untuk mengurangi risiko ini adalah dengan menerapkan teknik *Port Knocking* pada router MikroTik[7]. Teknik ini melibatkan mekanisme di mana port-port hanya akan terbuka setelah menerima serangkaian knocking atau sinyal tertentu, sehingga dapat mengurangi kemungkinan akses yang tidak sah. Dengan menggunakan simple *Port Knocking*, sistem dapat mendeteksi aktivitas mencurigakan dan mencegah serangan berbahaya sebelum dapat menembus jaringan, memastikan bahwa hanya pengguna yang sah yang memiliki akses[8].

Port Knocking adalah suatu sistem keamanan yang dirancang untuk membuka atau menutup akses ke port tertentu pada perangkat jaringan melalui penggunaan *firewall*[9]. Mekanisme ini dilakukan dengan cara mengirimkan paket atau koneksi yang spesifik. Tipe koneksi yang dimaksud dapat berupa protokol TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), atau ICMP (*Internet Control Message Protocol*)[10]. Oleh karena itu, untuk mendapatkan akses ke port tertentu yang telah dibatasi, pengguna diharuskan melakukan '*knocking*' terlebih dahulu dengan mengikuti serangkaian aturan yang hanya diketahui oleh pihak penyedia jaringan, yaitu administrator jaringan[11].

Pada penelitian ini *Filtering firewall* akan diterapkan pada CV Mitra Sukses Makmur. CV Mitra Sukses Makmur merupakan perusahaan yang bergerak dalam bidang penjualan grosir sembako. Sebagai perusahaan yang melayani berbagai jenis pelanggan, CV Mitra Sukses Makmur mengandalkan sistem jaringan yang andal untuk mendukung aktivitas operasionalnya,

seperti pengelolaan stok barang, transaksi penjualan, serta komunikasi internal dan eksternal. Namun, seiring dengan meningkatnya kebutuhan jaringan, perusahaan juga menghadapi tantangan dalam pengelolaan akses internet yang diberikan kepada karyawan.

Saat ini, CV Mitra Sukses Makmur telah menyediakan fasilitas Wi-Fi bagi karyawan untuk mendukung kelancaran pekerjaan. Namun, fasilitas tersebut sering kali disalahgunakan oleh beberapa karyawan untuk mengakses situs web yang tidak relevan, seperti media *social* milik pribadi dan platform streaming. Hal ini tidak hanya mengurangi efisiensi jaringan, tetapi juga menurunkan tingkat konsentrasi dan produktivitas karyawan. Dalam beberapa kasus, *Bandwidth* yang digunakan untuk aktivitas di luar pekerjaan juga mengganggu operasional penting perusahaan, seperti transaksi online dan akses ke sistem pengelolaan data.

Melihat permasalahan ini, CV Mitra Sukses Makmur memerlukan solusi yang efektif untuk membatasi akses internet tanpa mengorbankan kebutuhan operasional perusahaan. *Filtering firewall* berbasis MikroTik menjadi salah satu Solusi yang ditawarkan. *Filtering firewall* berbasis MikroTik mampu mengatur dan membatasi akses internet sesuai kebijakan perusahaan[6]. Dengan teknologi ini, Perusahaan diharapkan dapat memblokir situs atau aplikasi yang tidak relevan, mengatur prioritas *Bandwidth* untuk aktivitas penting, serta memantau penggunaan jaringan oleh karyawan.

Dengan implementasi *Filtering firewall*, diharapkan akses internet di CV Mitra Sukses Makmur dapat lebih terkontrol dan digunakan sesuai kebutuhan operasional. Selain meningkatkan keamanan jaringan, solusi ini juga diharapkan dapat membantu menciptakan lingkungan kerja yang lebih produktif, efisien, dan mendukung tercapainya tujuan perusahaan dalam jangka panjang. Filter yang diterapkan akan memastikan bahwa setiap karyawan menggunakan fasilitas internet secara bijak dan sesuai dengan kebijakan yang telah ditentukan, sehingga mendukung peningkatan kualitas kerja dan efektivitas operasional secara keseluruhan.

Dari pemaparan latar belakang di atas penulis mempunyai gagasan penelitian dengan judul **Implementasi *Filtering Firewall* Mikrotik pada CV Mitra Sukses Makmur**

1.2. Rumusan Masalah

Berdasarkan pemaparan dari latar belakang penelitian ini, beberapa rumusan maslah yang diidentifikasi adalah sebagai berikut:

1. Bagaimana mengimplementasikan jaringan *wireless* dan *firewall* Mikrotik pada CV. Mitra Sukses Makmur?
2. Bagaimana hasil konfigurasi kedua fitur Mikrotik tersebut saat digunakan para karyawan CV. Mitra Sukses Makmur?

1.3. Tujuan Penelitian

Dari dasar rumusan masalah, penelitian memiliki tujuan sebagai berikut:

1. Merancang Jaringan *Wireless* Mikrotik pada sistem informasi CV. Mitra Sukses Makmur.
2. Mengetauhi hasil akhir konfigurasi Mikrotik pada CV. Mitra Sukses Makmur

1.4. Batasan Penelitian

Penulis membatasi permasalahan yang ada pada penelitian ini sebagai berikut, untuk menghindari pembahasan Jaringan *Wireless* Mikrotik yang lebih luas:

1. Penelitian dilakukan pada CV. Mitra Sukses Makmur
2. Jaringan yang digunakan pada penelitian ini yaitu LAN (Local Area Network) dan WLAN (*Wireless* Local Area Network).
3. Membahas keamanan jaringan

1.5. Manfaat Penelitian

Tujuan penelitian ini adalah untuk memastikan jaringan beroperasi pada kapasitas terbaik, mengurangi lag, dan meningkatkan kecepatan koneksi internet. Serta memantau penggunaan jaringan secara realtime, dan melakukan troubleshooting secara cepat. Dengan manajemen jaringan yang baik dapat menghasilkan pekerjaan yang berkualitas dan lebih efisien dalam menyelesaikan tugas pada jam kerja.