

BAB I

PENDAHULUAN

1.1 Latar Belakang

Ada berbagai jenis serangan jaringan seperti serangan *browser*, serangan *Denial-of-Service* (DDoS), serangan cacing, dan beberapa serangan *malware*. Untuk mengatasi serangan jaringan tersebut, beberapa teknik telah disarankan (Shah et al., 2019). Keamanan jaringan di sekolah sangat penting karena jaringan yang tidak aman dapat menyebabkan masalah seperti virus atau *malware* yang dapat merusak sistem, dan akses ke konten yang tidak pantas atau tidak cocok untuk siswa. Sekolah harus memastikan bahwa jaringan mereka dilindungi dengan baik melalui penggunaan perangkat lunak keamanan yang mutakhir, pembaruan rutin sistem operasi dan aplikasi, serta kebijakan keamanan jaringan yang ketat. Keamanan jaringan Mikrotik juga penting untuk dijaga, karena MikroTik, merupakan salah satu perangkat jaringan yang sering digunakan untuk mengelola jaringan, bekerja dengan cara mengidentifikasi paket data yang hendak mengakses internet. Setelah diidentifikasi, perangkat ini akan memilih jalur penyedia layanan internet (ISP) yang akan digunakan (Amalia et al., 2023). MikroTik *RouterOS* adalah sistem operasi khusus yang digunakan pada

perangkat *router* jaringan, bertugas mengarahkan alamat di internet. Dengan menggunakan sistem operasi ini, kita mampu mengubah komputer di rumah menjadi *router*.

Layer 7 Protocol merupakan lapisan aplikasi yang bertindak sebagai perantara antar pengguna dengan aplikasi yang menggunakan jaringan, mengontrol akses pada jaringan yang kemudian menghasilkan pesan kesalahan (Husnaini et al., 2019). Protokol ini meliputi HTTP, FTP, DNS, dan sebagainya. Dengan mengidentifikasi jenis protokol yang digunakan, administrator jaringan dapat mengontrol akses ke internet dengan memblokir akses ke situs web yang tidak diinginkan.

Proxy server bisa diartikan sebagai perantara antara komputer klien dan jaringan internet. Semua permintaan akses dari klien ke internet harus melewati *proxy server* terlebih dahulu, sehingga memungkinkan pengelolaan akses dari klien saat berhubungan dengan internet (Putu et al., 2019). Dengan memanfaatkan *proxy server*, administrator jaringan memiliki kemampuan untuk mengendalikan akses internet dan menghalangi akses ke situs web yang tidak diinginkan. Selain itu, *proxy server* dapat digunakan untuk mempercepat akses internet dengan menyimpan data yang sering diakses dalam *cache*.

Dengan menggabungkan metode *Layer 7 Protocol* dan *Proxy Server*, administrator jaringan dapat membuat jaringan yang lebih aman dan efisien. Dalam perancangan keamanan ini, Mikrotik digunakan sebagai *router* dan *firewall*, sedangkan *proxy server* digunakan untuk mengontrol akses ke internet dan mempercepat akses internet. Dengan menggunakan teknik ini, administrator jaringan diharapkan dapat melindungi jaringan dari serangan luar dan mengontrol akses ke internet secara efektif.

Berdasarkan penelitian tentang “Manajemen *Proxy* Menggunakan Mikrotik dengan Metode *Layer 7 Protocol* dan *Mangle*” (Azmi, 2022) diterangkan bahwa penelitian ini telah berhasil melakukan pemblokiran pada situs yang di inginkan dengan akurasi 100% melalui *url* dan bukan dari *search engine*. Dengan ini hasil pemblokiran kurang maksimal dan hanya terpaku pada alamat yang di masukkan atau bisa dibilang kurang *flexible*.

Berdasarkan uraian diatas, penulis memiliki ide untuk membuat sebuah penelitian dengan judul “Perancangan Keamanan Menggunakan Mikrotik dengan Metode *Layer 7 Protocol* dan *Proxy Server*” yang ditujukan pada jaringan internet sekolah dengan harapan,

semoga siswa siswi yang menggunakan jaringan internet di sekolah ini dapat merasa aman dan nyaman.

1.2 Rumusan Masalah

Dari latar belakang yang diuraikan terdapat rumusan masalah sebagai berikut:

1. Bagaimana cara kerja *layer 7 protocol* dalam mengamankan jaringan ?
2. Bagaiaman cara *proxy server* digunakan untuk memperkuat keamanan jaringan ?
3. Bagaimana cara mengimplementasika metode *layer 7 protocol* dan *proxy server* dalam perancangan keamanan dengan menggunakan mikrotik ?

1.3 Tujuan Penelitian

Adapun tujuannya sebagai berikut:

1. Meningkatkan kinerja secara keseluruhan dengan menggunakan *Layer 7 Protocol*.
2. Memberikan lapisan tambahan keamanan dengan menganalisis lalu lintas jaringan dan memfilter konten yang tidak diinginkan. Dengan menerapkan *proxy server*.
3. Mengimplementasikan sistem keamanan yang telah dirancang dan melakukan uji coba untuk memastikan bahwa sistem tersebut dapat berfungsi dengan baik dengan *Layer 7 Protocol* dan *Proxy Server*.

1.4 Manfaat Penelitian

1. Meningkatkan keamanan jaringan *wireless*
2. Meningkatkan efisiensi pengelolaan jaringan
3. Menjadi rujukan bagi pihak yang memerlukan informasi terkait perancangan keamanan menggunakan mikrotik dengan metode *layer 7 protocol* dan *proxy server*.

1.5 Batasan Masalah

Batasan masalah dari perancangan keamanan menggunakan Mikrotik dengan metode *Layer 7 Protocol* dan *Proxy Server* dapat dijabarkan sebagai berikut:

1. Perancangan ini hanya difokuskan pada implementasi Mikrotik sebagai perangkat jaringan untuk meningkatkan keamanan jaringan di sekolah dan tidak diperuntukkan pada pemakaian *vpn*.
2. Metode yang akan digunakan dalam perancangan ini adalah *Layer 7 Protocol* dan *Proxy Server*.
3. Pengujian ini akan dibatasi pada jaringan lokal yang terdiri dari beberapa komputer yang terhubung ke Mikrotik melalui jaringan kabel atau nirkabel.