202110370311507
M. Rizqi Dwi Adi Saputro
Prodi Informatika

BAB I

PENDAHULUAN

1.1 Latar Belakang

Mikrotik RouterOS merupakan system operasi berbasis Linux yang sangat populer dan banyak digunakan sebagai solusi router dan firewall karena fleksibilitas, fitur yang lengkap, dan harga yang terjangkau. Mikrotik juga menyediakan sistem manajemen jaringan yang komprehensif, yang memungkinkan administrator untuk mengelola lalu lintas data, mengontrol aliran data masuk dan keluar berdasarkan aturan yang ditetapkan untuk penerapan kebijakan keamanan secara efisien. Menurut Pratomo MikroTik RouterOS menyediakan fitur firewall yang lengkap dan dapat dikembangkan menjadi sistem keamanan yang lebih kompleks, sehingga secara signifikan meningkatkan perlindungan jaringan terhadap ancaman eksternal [1]. Selain itu, penelitian oleh Maulana menunjukan bahwa penerapan firewall pada MikroTik terbukti efektif dalam membatasi akses ke situs web tertentu dan mencegah serangan DoS (Denial of Service), dengan performa CPU yang tetap stabil di kisaran 1% saat diuji menggunakan aplikasi LOIC [2]. Hal ini menunjukkan bahwa MikroTik tidak hanya unggul dari segi konfigurasi dan fleksibilitas, tetapi juga dari sisi efisiensi sumber daya dan kemampuan mitigasi ancaman jaringan.

Namun, dalam praktiknya pengelolaan akses jaringan masih sering mengalami kendala. Beberapa pengguna mencoba mengakses sumber daya jaringan tanpa izin atau menggunakan bandwidth secara berlebihan sehingga menggangu pengguna lain. Selain itu, tanpa adanya sistem *monitoring* yang baik, administrator jaringan sering kali terlambat mengetahui ketika terjadi pelanggaran atau ancaman terhadap sistem. Kurangnya implementasi sistem *monitoring real-time* dan kebijakan manajemen bandwidth yang baik dapat memperbesar peluang terjadinya penyalahgunaan akses jaringan dan serangan internal yang sulit terdeteksi [3]. Pemantauan secara langsung terhadap trafik

memungkinkan administrator untuk mendeteksi anomali dan gangguan dengan cepat serta mengambil langkah mitigasi yang tepat sebelum ancaman berkembang lebih jauh [4]. Tanpa adanya pembatasan bandwidth beban trafik bisa meningkat drastis dan menyebabkan gangguan kinerja secara menyeluruh dalam jaringan [5]. Hal ini menyebabkan risiko keamanan yang tinggi dan menurunkan performa jaringan secara keseluruhan.

Menjawab permasalahan tersebut, Mikrotik menyediakan teknologi packet filtering sebagai solusi utama dalam mengatur dan membatasi lalu lintas. Sistem packet filtering yang diterapkan melalui perangkat MikroTik dapat secara efisien menyaring dan menghentikan penyebaran paket berbahaya seperti virus *worm*, berkat konfigurasi aturan firewall yang tepat sebelumnya [6]. Packet filtering adalah mekanisme fundamental dalam pengelolan jaringan yang memungkinkan kontrol aliran data masuk dan keluar. Fungsi utama dari packet filtering adalah memeriksa *header* setiap paket data yang melintas dan membandingkannya dengan aturan yang telah ditetapkan. Pemanfaatan fitur filtering pada MikroTik memungkinkan penyaringan lalu lintas jaringan dari level protokol dasar hingga layer aplikasi, termasuk memblokir akses ke konten yang tidak sesuai seperti situs dewasa [7]. Melalui proses ini packet filtering secara efektif dapat memblokir lalu lintas sesuai yang ditetapkan oleh administrator seperti memblokir lalu lintas yang tidak diinginkan, mencegah akses tidak sah, dan melindungi sumber daya jaringan dari berbagai ancaman siber. Fitur firewall yang terdapat pada MikroTik sangat efektif dalam menangkal sebagian besar lalu lintas serangan DDoS, dengan keberhasilan pemblokiran mencapai lebih dari 70%, sekaligus mengurangi tekanan kinerja CPU.

Dalam penerapan packet filtering, dibutuhkan metode yang tidak hanya membatasi lalu lintas tetapi juga mampu memantau aktivitas jaringan secara langsung. Salah satu metode yang digunakan dalam penelitian ini adalah mengintegrasikan packet filtering dengan Bot Telegram. Integrasi ini memungkinkan sistem untuk mendeteksi pola lalu lintas jika terdapat aktivitas yang mencurigakan atau melanggar aturan jaringan telegram bot akan

berfungsi sebagai media notifikasi untuk memberitahu administrator. Packet filtering pada MikroTik dengan fitur notifikasi lewat Telegram dapat secara *real-time* memperingatkan administrator jika terjadi pelanggaran kebijakan akses internet seperti upaya pengaksesan situs[8]. Bot telegram memungkinkan untuk melakukan monitoring aktivitas serangan jaringan seperti DDoS, upaya login illegal dan *port scanning,* kemudian mengirimkan notifikasi yang berisi log[9].

Beberapa penelitian sebelumnya menunjukkan bahwa penerapan packet filtering pada MikroTik efektif dalam pengelolaan dan pengamanan jaringan. Penelitian oleh Susanto dan teman-temanya membuktikan bahwa kombinasi packet filtering dan application layer gateway mampu membatasi akses ke situs tertentu serta menurunkan akses ke situs terlarang hingga 100%[10]. Penelitian oleh Melkov dan teman-temanya menemukan bahwa iptables memiliki performa yang lebih stabil dan throughput tinggi dalam pengelolaan aturan filtering skala besar[11]. Penelitian oleh Ria dan teman-temanya menunjukkan bahwa integrasi Telegram Bot mampu memberikan notifikasi real-time terhadap gangguan perangkat jaringan[12], sementara Penelitian oleh Suhardono dan teman-temanya membuktikan bahwa packet filtering yang dikombinasikan dengan notifikasi Telegram efektif dalam memantau dan membatasi akses internet, dengan waktu respons notifikasi berkisar antara 23 hingga 26,9 detik[8].

Namun, dari keempat penelitian tersebut, masih terdapat celah dalam hal otomatisasi *monitoring* secara *real-time* terhadap aktivitas jaringan yang melanggar kebijakan akses. Penelitian oleh Susanto dan teman-temanya lebih fokus pada efisiensi packt filtering dan pengendalian akses tanpa menyentuh aspek notifikasi otomatis[10]. Sementara penelitian Melkov dan temannya berfokus pada performa filtering di sistem Linux, bukan MikroTik secara spesifik[11]. Penelitian oleh Ria dan temannya memang telah mengimplementasikan notifikasi *real-time* menggunakan Telegram Bot, namun lebih berfokus kearah pemantauan status perangkat dan belum mengintegrasikan packet filtering sebagai mekanisme pembatasan akses serta

simulasi dari serangan DDoS[12]. Sementara itu, penelitian Suhardono dan temanya sudah memadukan packet filtering dengan Telegram Bot, tetapi masih terbatas pada skenario pemblokiran situs dan game online tanpa pengujian dalam kondisi serangan ekstrem seperti DDoS[8].

Dengan demikian, belum adanya penelitian yang secara komprehensif menggabungkan fungsi pembatasan akses menggunakan packet filtering di MikroTik dengan sistem notifikasi otomatis berbasis Telegram Bot untuk memantau serangan jaringan secara langsung. Penelitian ini dibuat untuk mengisi masalah tersebut dengan membangun sistem monitoring yang tidak hanya membatasi, tetapi juga mampu memberikan peringatan instan kepada administrator ketika terjadi aktivitas mencurigakan atau pelanggaran aturan akses jaringan.

1.2 Rumusan Masalah

1. Bagaimana mengintegrasikan notifikasi *real-time* dari MikroTik ke bot Telegram untuk memantau aktivitas pembatasan akses jaringan?
2. Seberapa efektif kombinasi Packet Filtering pada MikroTik dan integrasi bot Telegram dalam meningkatkan kemampuan *monitoring* dan pembatasan akses jaringan?

1.3 Tujuan Penelitian

1. Membangun sistem integrasi antara MikroTik dan bot Telegram untuk mengirimkan notifikasi *real-time* mengenai aktivitas pembatasan akses jaringan kepada administrator.
2. Menganalisis efektivitas sistem *monitoring* dan pembatasan akses jaringan yang dihasilkan dari kombinasi Packet Filtering pada MikroTik dan integrasi bot Telegram.

1.4 Batasan Penelitian

1. Integrasi notifikasi hanya akan dilakukan melalui platform Telegram menggunakan bot Telegram. Platform komunikasi lain tidak akan menjadi bagian dari penelitian ini.

2. Pembatasan akses akan difokuskan pada pemblokiran situs web (berdasarkan domain atau IP) dan mungkin layanan tertentu (berdasarkan port/protokol), sesuai dengan kemampuan Packet Filtering.
3. Simulasi DDOS hanya pada pengiriman mengirimkan paket dengan jumlah besar ke Mikrotik.
4. Monitoring akan terbatas pada notifikasi terkait aktivitas yang diblokir oleh aturan Packet Filtering, bukan monitoring performa jaringan secara keseluruhan atau deteksi intrusi yang lebih kompleks.
5. Fokus utama penelitian ini secara eksklusif pada metode Packet Filtering.