202110370311507
M. Rizqi Dwi Adi Saputro
Prodi Informatika

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Beberapa penelitian sebelumya dapat dilihat pada table 2.1

Tabel 2.1 Penelitian Terdahulu

NO	Judul	Penulis	Metode	Pembahasan
1	Packet Filtering Gateway and Application Layer Gateway on Mikrotik Router Based Firewalls for Server and Internet Access Restrictions	Susanto et al. (2023)	Packet Filtering + NDLC	Pemfilteran packet alamat IP dalam sistem firewall yang bekerja pada tingkat jaringan dengan memeriksa alamat IP sumber dan tujuan dari setiap paket. Tujuannya adalah untuk mengizinkan atau memblokir akses berdasarkan aturan yang telah ditetapkan, sehingga hanya paket dari alamat IP tertentu yang diizinkan melewati firewall.

2	Performance Testing of Linux Firewalls	Melkov et al. (2020)	Packet Filtering	pengujian performa firewall Linux, khususnya iptables dan nftables, menunjukkan bahwa pengujian dilakukan dengan menggunakan metodologi packet filtering. Pengujian ini bertujuan untuk mengukur performa filter paket dalam berbagai kondisi, seperti jumlah aturan yang diterapkan dan konfigurasi sumber daya virtual (vCPU)
3	Implementation Of Telegram Bot Notification On Network Device Monitoring System	Ria et al. (2024)	Bot Telegram + NDLC	Pembahasan terkait implementasi sistem monitoring berbasis Telegram Bot menunjukkan bahwa langkah

				awal yang penting adalah konfigurasi jaringan dan perangkat yang digunakan. Pada tahap awal, jaringan diambil dari ISP melalui Routerboard yang sudah memiliki fitur wireless, kemudian diatur dalam mode station untuk mengakses internet secara langsung.
4	Teknik Keamanan Akses Internet Untuk Parenting Menggunakan Metode Packet Filtering Pada Mikrotik	Suhardono et al. (2023)	Packet Filtering + Bot Telegram	Penelitian ini membangun sistem keamanan akses internet untuk parental control dengan menggunakan metode packet filtering pada MikroTik yang diintegrasikan dengan notifikasi bot Telegram. Tujuannya adalah

	memblokir situs/media sosial/game online tertentu dan mengirimkan peringatan secara otomatis ketika terjadi pelanggaran akses.

2.2 Mikrotik RouterOS

Mikrotik RouterOS adalah sistem berbasis linux yang dirancang khusus untuk mengelola jaringan dan menyediakan fitur seperti routing statis, routing dinamis, firewall, *hotspot, bandwidth, DHCP, cache DNS, proxy web*, dan VPN [13]. Mikrotik mampu mengelola routing jaringan komputer yang memungkinkan analisis kinerja yang efisien dan kontrol atas akses internet dan kebijakan keamanan [14]. Salah satu keunggulan Mikrotik adalah kemampuanya dalam menerapkan firewall berbasis packet filtering untuk menyaring lalu lintas jaringan. Mikrotik RouterOS banyak digunakan oleh administrator jaringan karena memiliki GUI yang lebih mudah melalui aplikasi WInbox, membuatnya ramah pengguna [15].

2.3 Packet Filtering

Packet Filtering adalah Teknik penyaringan paket data berdasarkan parameter tertentu, seperti Alamat IP sumber atau tujuan untuk mencegah akses ke situs dan aplikasi yang tidak diinginkan [16]. Penyaringan paket menggunakan Mikrotik adalah metode penting untuk meningkatkan keamanan jaringan. Penyaringan paket berpotensi untuk mengurangi risiko yang terkait dengan perangkat yang dikompromikan[17].

2.4 Firewall

Firewall dalam fitur Mikrotik RouterOS menawarkan fitur yang komprehensif. Hal ini digunakan untuk meningkatkan keamanan jaringan dengan menerapkan sistem firewall yang kompleks, yang mencakup pemblokiran akses, pembatasan bandwidth, dan memiliki kemampuan untuk memantau perlindungan data dengan baik [18]. Firewall MikroTik menggunakan pemfilteran paket melalui aturan Raw dan filter untuk membatasi akses ke situs web tertentu dan mencegah serangan DoS [19].

2.5 Serangan DDOS

Distributed Denial of Service (DDoS) adalah serangan yang membanjiri bandwidth atau sumber daya target supaya mengakibatkan penolakan layanan bagi pengguna yang sah untuk memperlambat atau merusak sistem target[20]. Serangan DDoS sering kali terjadi untuk mengeksploitasi atau mengganggu lalu lintas sistem sehingga banyak peneliti yang melakukan simulasi serta pencegahan serangan DDos [21].

2.6 Monitoring Trafik Jaringan

Pemantauan jaringan melibatkan alat untuk memantau kinerja jaringan dan memastikan pemantauan yang efektif [22]. Pemantauan jaringan sangat penting untuk mengatasi dan mendeteksi ancaman siber atau aktivitas yang mencurigakan [23].

2.7 Bot Telegram untuk Notifikasi Jaringan

Telegram Bot digunakan untuk manajemen dan pemantauan jaringan, memungkinkan administrator jaringan untuk mengelola perangkat MikroTik dari jarak jauh[24]. Telegram Bot dapat memberikan peringatan secara real-time dari sistem untuk mendeteksi serangan yang dikirimkan ke administrator jaringan [25].

2.8 QoS

Quality of Service (QoS) merupakan parameter pengukuran yang digunakan untuk mengukur seberapa baik kinerja jaringan[26] Parameter yang digunakan untuk pengukuran agar memperoleh informasi mengenai kualitas

jaringan melalui parameter penting seperti *Througput, Delay,* dan *Packet Loss* [27]. Selain itu, proses evaluasi dilakukan dengan menerapkan rumus-rumus perhitungan QoS untuk memastikan bahwa setiap parameter jaringan diukur secara sistematis [28]

2.8.1 Throughput

Throughput atau jumlah ukuran data yang berhasil dikirimkan dan diterima melalui jaringan dalam satu [29]. Parameter ini menggambarkan seberapa besar kapasitas jaringan dalam mentransmisikan data selama proses komunikasi berlangsung. Nilai *throughput* dihitung menggunakan rumus:

$$Throughput = \frac{\text{Paket data diterima}}{\text{Lama Pengamatan}} \quad \textbf{(1)}$$

2.8.2 Delay

Delay atau waktu yang diperlukan paket data untuk berpindah dari pengiriman menuju penerima [30]. Parameter ini menunjukan tingkat kecepatan jaringan dalam mengantarkan paket data selama proses komunikasi berlangsung. Nilai dari *delay* dapat dihitung menggunakan rumus :

$$Delay = \frac{\sum \text{ delay per paket}}{Total\ Paket} \quad \textbf{(2)}$$

2.8.3 Packet Drop

Packet drop atau packet loss menggambarkan jumlah paket yang gagal untuk mencapai tujuan [31]. Parameter ini menunjukan tingkat keandalan jaringan dalam menjaga agar seluruh paket dapat ditransmisikan dengan baik. Nilai dari *packet drop* dapat dihitung menggunakan rumus :

$$Packet\ Loss = \frac{(\text{Paket data dikirim} - \text{Paket data diterima})}{\text{Paket data dikirim}} x100\% \quad \textbf{(3)}$$