Analisis Efektivitas *Firewall MikroTik* dalam Mitigasi Serangan *DDoS* menggunakan Pendekatan *Network Development Life Cycle* (NDLC)

Analysis of MikroTik Firewall Effectiveness in Mitigating DDoS Attacks using the Network Development Life Cycle (NDLC) Approach

[1]M. Irsyadul 'ibad*, [2]Wildan Mahmud, [3]Galuh Wilujeng
[1,2,3]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro PSDKU Kediri
[1,2,3]Jl.Penanggungan No 41A, Bandar Lor, Kec. Mojoroto, Kota Kediri, Jawa Timur, Indonesia
*e-mail: 612202400162@mhs.dinus.ac.id

(***received*:** 23 April 2026, ***revised*:** 6 May 2026, ***accepted*:** 7 May 2026)

Abstrak

Penelitian ini dilatarbelakangi oleh meningkatnya ancaman keamanan jaringan seiring dengan berkembangnya layanan berbasis digital pada instansi pemerintah. Salah satu serangan yang sering terjadi adalah Distributed Denial of Service (DDoS) yang dapat menyebabkan degradasi performa jaringan dan gangguan layanan. Penelitian ini bertujuan untuk menganalisis efektivitas implementasi firewall MikroTik dalam memitigasi serangan DDoS pada jaringan Diskominfo Kota Kediri menggunakan metode Network Development Life Cycle (NDLC). Tahapan penelitian meliputi analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Pengujian dilakukan dengan mensimulasikan serangan SYN Flood menggunakan aplikasi Hping3 serta mengukur parameter yang digunakan meliputi throughput, delay, packet loss, serta penggunaan CPU pada router. Hasil pengujian menunjukkan bahwa pada kondisi serangan DDoS tanpa firewall, throughput meningkat hingga ±40 Mbps, delay mencapai 5–15 ms, packet loss sebesar ±20–30%, serta penggunaan CPU meningkat hingga 99–100%. Setelah firewall diimplementasikan, performa jaringan mengalami perbaikan signifikan dengan throughput menurun menjadi ±2 Mbps, delay kembali stabil di bawah 1 ms, packet loss menjadi 0%, serta penggunaan CPU turun menjadi ±3%. Hasil tersebut menunjukkan bahwa firewall MikroTik efektif dalam memfilter trafik tidak normal serta mengurangi beban sistem, sehingga mampu meningkatkan stabilitas jaringan dan menjaga kualitas layanan berdasarkan parameter Quality of Service (QoS).

Kata Kunci: DDoS, NDLC, keamanan jaringan, firewall MikroTik, SYN flood

Abstract

This study is motivated by the increasing network security threats accompanying the growth of digital-based services in government institutions. One of the most common threats is the Distributed Denial of Service (DDoS) attack, which can cause network performance degradation and service disruption. This research aims to analyze the effectiveness of implementing a MikroTik firewall in mitigating DDoS attacks on the network of the Diskominfo Kota Kediri using the Network Development Life Cycle (NDLC) method. The research stages consisted of analysis, design, simulation, implementation, monitoring, and management. The testing process was conducted by simulating SYN Flood attacks using the Hping3 application. The evaluated parameters included throughput, delay, packet loss, and CPU utilization on the router. The experimental results showed that under DDoS attack conditions without firewall protection, throughput increased to approximately 40 Mbps, delay reached 5–15 ms, packet loss ranged from approximately 20–30%, and CPU utilization increased to 99–100%. After the firewall was implemented, network performance improved significantly, with throughput decreasing to approximately 2 Mbps, delay stabilizing below 1 ms, packet loss reduced to 0%, and CPU utilization decreasing to approximately 3%. These findings indicate that the MikroTik firewall is effective in filtering abnormal traffic and reducing system load,

 ISSN:2302-8149
e-ISSN:2540-9719

thereby improving network stability and maintaining service quality based on Quality of Service (QoS) parameters.

***Keywords**: DDoS, NDLC, network security, mikrotik firewall, SYN flood*

1. Pendahuluan

Perkembangan teknologi informasi dalam beberapa tahun terakhir telah mendorong instansi pemerintah untuk bertransformasi menuju layanan berbasis digital melalui konsep *e-government*. Transformasi ini bertujuan untuk meningkatkan efisiensi dan kualitas pelayanan publik serta memberikan akses yang lebih cepat dan transparan kepada masyarakat. Di Indonesia, implementasi sistem pemerintahan berbasis elektronik telah diatur melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai landasan dalam pengelolaan sistem digital di lingkungan pemerintahan [1]. Selain itu, Badan Siber dan Sandi Negara (BSSN) memiliki peran penting dalam menjaga keamanan siber nasional, termasuk perlindungan infrastruktur jaringan pemerintah [2].

Seiring dengan meningkatnya penggunaan layanan digital, ancaman terhadap keamanan jaringan juga semakin kompleks. Salah satu ancaman yang sering terjadi adalah serangan *Distributed Denial of Service* (DDoS), yaitu serangan yang dilakukan dengan membanjiri jaringan menggunakan trafik dalam jumlah besar sehingga menyebabkan penurunan performa hingga layanan tidak dapat diakses [3]. Pada lingkungan jaringan modern seperti *cloud computing* dan *software-defined network*, serangan ini menjadi semakin kompleks dan sulit ditangani karena melibatkan pola trafik yang dinamis [4].

Untuk mengatasi permasalahan tersebut, firewall menjadi salah satu solusi utama dalam sistem keamanan jaringan. Firewall berfungsi untuk mengontrol lalu lintas data, membatasi akses yang tidak sah, serta memfilter trafik berbahaya [5]. Implementasi firewall berbasis MikroTik telah banyak digunakan untuk meningkatkan keamanan jaringan serta mengelola trafik secara lebih efektif [6]. Selain itu, penerapan firewall juga terbukti mampu meningkatkan stabilitas jaringan serta mengurangi dampak serangan berbasis trafik [7].

Meskipun demikian, efektivitas implementasi firewall dalam kondisi jaringan nyata masih sangat bergantung pada bagaimana sistem tersebut diterapkan dan diuji pada lingkungan operasional yang sesungguhnya. Oleh karena itu, diperlukan pengujian langsung pada jaringan yang digunakan dalam aktivitas layanan publik untuk mengetahui sejauh mana sistem keamanan tersebut mampu bekerja secara optimal.

Dalam konteks implementasi di lapangan, jaringan pada Diskominfo Kota Kediri digunakan untuk mendukung berbagai layanan digital pemerintahan, seperti pengelolaan informasi publik, layanan administrasi berbasis sistem, serta konektivitas antar perangkat kerja di lingkungan instansi. Ketersediaan jaringan yang stabil menjadi faktor penting karena layanan tersebut digunakan secara berkelanjutan dalam aktivitas operasional sehari-hari.

Namun, berdasarkan hasil observasi, sistem keamanan jaringan yang digunakan masih memiliki keterbatasan dalam menangani lonjakan trafik yang tidak normal. Kondisi ini terlihat ketika terjadi peningkatan trafik secara tiba-tiba yang berpotensi menyebabkan penurunan performa jaringan, bahkan dapat mengganggu akses layanan. Tanpa adanya mekanisme filtering yang optimal, seluruh trafik akan diproses secara langsung oleh router sehingga meningkatkan beban kerja sistem secara signifikan. Kondisi serupa juga ditemukan pada penelitian sebelumnya yang menunjukkan bahwa sistem keamanan jaringan tanpa mekanisme filtering yang memadai cenderung mengalami penurunan performa ketika terjadi lonjakan trafik [8]. Selain itu, implementasi firewall yang belum optimal dapat menyebabkan jaringan tidak mampu mengontrol trafik secara efektif [9]. Penelitian lain juga menyebutkan bahwa keterbatasan dalam pengelolaan trafik dapat meningkatkan risiko gangguan layanan jaringan [10].

Meskipun berbagai penelitian telah mengkaji implementasi firewall maupun metode deteksi serangan berbasis *machine learning*, sebagian besar penelitian tersebut masih berfokus pada satu pendekatan tertentu tanpa mengintegrasikan proses pengembangan jaringan secara menyeluruh [8]. Selain itu, pengujian yang dilakukan umumnya hanya menitikberatkan pada satu kondisi jaringan tanpa memberikan perbandingan yang jelas antara kondisi sebelum dan sesudah penerapan sistem keamanan [9]. Penelitian lain juga menunjukkan bahwa analisis performa jaringan sering kali belum

 ISSN:2302-8149
e-ISSN:2540-9719

dilakukan secara komprehensif menggunakan parameter *Quality of Service* (QoS) seperti throughput, delay, dan packet loss secara bersamaan [10].

Dengan demikian, terdapat celah penelitian (research gap) berupa belum adanya pendekatan terintegrasi yang menggabungkan implementasi firewall dengan metode pengembangan jaringan secara sistematis, serta analisis performa jaringan secara kuantitatif berdasarkan parameter QoS dalam berbagai kondisi pengujian.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengimplementasikan firewall MikroTik menggunakan metode *Network Development Life Cycle* (NDLC) serta mengevaluasi efektivitasnya dalam memitigasi serangan DDoS melalui pengukuran parameter QoS, yaitu throughput, delay, dan packet loss. Pengujian dilakukan dalam tiga kondisi, yaitu kondisi normal, saat terjadi serangan, dan setelah penerapan firewall, sehingga diperoleh gambaran yang lebih komprehensif terhadap performa jaringan.

2. Tinjauan Literatur

Penelitian terkait keamanan jaringan menunjukkan bahwa serangan *Distributed Denial of Service* (DDoS) masih menjadi ancaman utama yang dapat mengganggu stabilitas layanan jaringan karena mampu membanjiri sistem dengan trafik dalam jumlah besar [3]. Seiring dengan berkembangnya teknologi jaringan modern, karakteristik serangan menjadi semakin kompleks dan sulit dideteksi secara konvensional [4]. Kondisi ini menunjukkan bahwa sistem keamanan jaringan membutuhkan mekanisme yang tidak hanya mampu mendeteksi serangan, tetapi juga mengendalikan trafik secara efektif.

Berbagai penelitian telah mengkaji implementasi firewall sebagai mekanisme utama dalam pengamanan jaringan. Firewall berperan dalam mengontrol lalu lintas data serta memfilter trafik yang berpotensi berbahaya sehingga dapat meningkatkan keamanan sistem secara signifikan [5]. Implementasi firewall berbasis MikroTik menunjukkan hasil yang efektif dalam mengelola trafik jaringan serta membatasi akses yang tidak sah [6]. Selain itu, konfigurasi firewall yang tepat mampu meningkatkan stabilitas jaringan serta mengurangi dampak serangan DDoS[11]. Hal ini menunjukkan bahwa firewall tidak hanya berfungsi sebagai sistem proteksi, tetapi juga sebagai mekanisme kontrol yang berpengaruh langsung terhadap performa jaringan.

Penelitian lain menunjukkan bahwa penerapan firewall pada router MikroTik mampu mengamankan jaringan dari serangan DoS melalui mekanisme filtering yang optimal [10]. Selain itu, implementasi firewall juga dapat digunakan untuk mengantisipasi serangan jaringan melalui pengaturan akses yang lebih terstruktur [12]. Penggunaan metode firewall filtering pada perangkat MikroTik terbukti memberikan fleksibilitas dalam pengelolaan trafik jaringan [13]. Pengembangan sistem keamanan jaringan berbasis firewall juga mampu meningkatkan kontrol terhadap akses jaringan secara signifikan [14]. Implementasi keamanan jaringan berbasis MikroTik pada berbagai lingkungan juga menunjukkan peningkatan performa dan stabilitas jaringan setelah konfigurasi dilakukan secara optimal [15]. Selain itu, penggunaan metode firewall dalam pengamanan jaringan komputer terbukti mampu meningkatkan efektivitas perlindungan sistem dari ancaman jaringan[16]. Penelitian lain juga menunjukkan bahwa firewall MikroTik efektif diterapkan pada instansi pemerintah dalam meningkatkan keamanan jaringan secara menyeluruh [17]. Temuan-temuan tersebut mengindikasikan bahwa efektivitas firewall sangat dipengaruhi oleh konfigurasi serta penerapan yang sesuai dengan kondisi jaringan.

Pengembangan metode keamanan jaringan juga mencakup pendekatan tambahan seperti *intrusion detection system* dan metode berbasis *machine learning*. Pendekatan ini memungkinkan sistem untuk mendeteksi pola serangan secara lebih adaptif dan akurat pada lingkungan jaringan dengan trafik dinamis. Penelitian lain menunjukkan bahwa metode berbasis *machine learning* mampu meningkatkan akurasi deteksi serangan DDoS secara signifikan [18]. Selain itu, pendekatan berbasis *deep learning* juga digunakan untuk meningkatkan efektivitas deteksi serangan pada jaringan modern [19]. Metode lain menunjukkan bahwa teknik pembelajaran mesin mampu mendeteksi serangan DDoS dengan tingkat akurasi yang tinggi [20]. Pendekatan berbasis *deep learning* juga memberikan peningkatan performa dalam mendeteksi serangan pada sistem jaringan skala besar [21]. Meskipun demikian, penerapan metode tersebut umumnya memerlukan sumber daya komputasi yang lebih besar dibandingkan dengan pendekatan berbasis firewall.

 ISSN:2302-8149
e-ISSN:2540-9719

Selain aspek keamanan, beberapa penelitian juga menekankan pentingnya pendekatan yang terstruktur dalam pengembangan jaringan. Metode *Network Development Life Cycle* (NDLC) memberikan tahapan sistematis mulai dari analisis, desain, simulasi, implementasi, monitoring, dan hingga manajemen sehingga implementasi jaringan dapat dilakukan secara lebih terarah [9]. Pendekatan ini memungkinkan integrasi antara perancangan sistem keamanan dan evaluasi performa jaringan dalam satu kerangka kerja yang sistematis.

Berdasarkan berbagai penelitian tersebut, dapat disimpulkan bahwa firewall memiliki peran penting dalam menjaga keamanan jaringan. Namun, implementasi yang efektif tidak hanya bergantung pada penggunaan firewall semata, tetapi juga membutuhkan pendekatan yang terstruktur serta pengujian langsung pada kondisi jaringan nyata agar hasil yang diperoleh lebih relevan dengan kebutuhan di lapangan.

3. Metode Penelitian

Penelitian ini dilakukan dengan pendekatan eksperimen yang berfokus pada pengujian langsung terhadap performa jaringan sebelum dan sesudah implementasi firewall. Pendekatan ini dipilih agar hasil yang diperoleh dapat menggambarkan kondisi nyata di lingkungan jaringan yang diteliti.

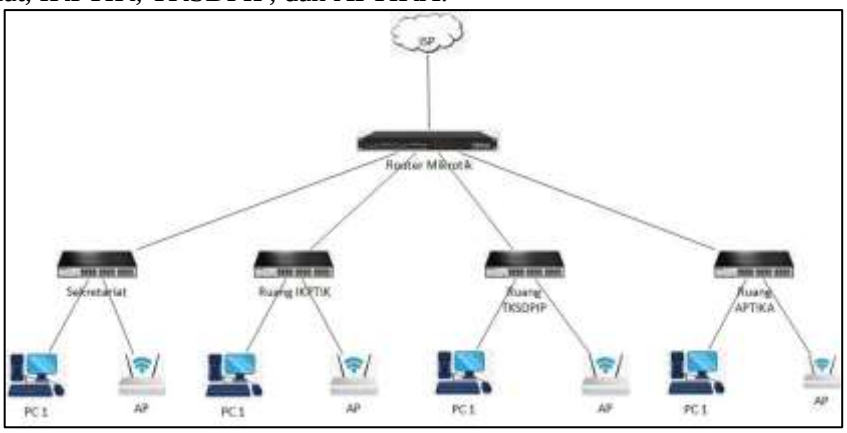
Penelitian ini menggunakan metode Network Development Life Cycle (NDLC) untuk merancang, mengimplementasikan, dan mengevaluasi sistem keamanan jaringan. Metode ini dipilih karena mampu memberikan tahapan yang sistematis dalam pengembangan jaringan, mulai dari analisis hingga evaluasi.

3.1 Objek Penelitian

Objek penelitian ini adalah jaringan komputer pada Diskominfo Kota Kediri yang digunakan untuk mendukung layanan berbasis digital. Jaringan tersebut terdiri dari beberapa segmen, yaitu Sekretariat, TKSDPIP, IKPTIK, dan APTIKA yang terhubung melalui router MikroTik sebagai pusat pengendali jaringan.

3.2 Rancangan dan Teknik Pengumpulan Data

Penelitian ini dilakukan dengan merancang topologi jaringan yang merepresentasikan kondisi jaringan nyata di lingkungan Diskominfo. Topologi yang digunakan terdiri dari satu router MikroTik sebagai pusat pengendali jaringan yang terhubung langsung dengan sumber internet (ISP). Router tersebut kemudian mendistribusikan koneksi ke beberapa segmen jaringan yang berbeda, yaitu Sekretariat, IKPTIK, TKSDPIP, dan APTIKA.



Gambar 1 Topologi jaringan

Berdasarkan Gambar 1 seluruh trafik jaringan internal akan melewati router MikroTik sebelum menuju jaringan eksternal (internet). Kondisi ini mengindikasikan bahwa router MikroTik berperan sebagai pusat pengendali jaringan yang bertugas mengatur serta memfilter seluruh lalu lintas data. Dengan posisi tersebut, router menjadi titik strategis dalam penerapan sistem keamanan, khususnya dalam mengidentifikasi dan mengendalikan trafik yang tidak normal.

Untuk mendukung proses pengujian, digunakan skema pengalamatan IP yang terstruktur sebagaimana ditunjukkan pada Tabel 1.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 1 Skema alamat ip jaringan

No	Nama Jaringan	Network IP	Gateway	Keterangan
1	ISP	103.xxx.xxx.xxx/29	103.xxx.xxx.xxx	Koneksi ke internet
2	MikroTik	103.xxx.xxx.xxx/29	103.xxx.xxx.xxx	Interface ke ISP
3	Sekretariat	10.10.1.0/24	10.10.1.1	Jaringan lokal Sekretariat
4	TKSDPIP	192.168.12.0/24	192.168.12.1	Jaringan lokal TKSDPIP
5	IKPTIK	192.168.13.0/24	192.168.13.1	Jaringan lokal IKPTIK
6	APTIKA	192.168.11.0/24	192.168.11.1	Jaringan lokal APTIKA

Teknik pengumpulan data dilakukan dengan melakukan pengujian jaringan dalam tiga kondisi, yaitu kondisi normal, saat terjadi serangan DDoS, dan setelah penerapan firewall. Serangan DDoS disimulasikan menggunakan aplikasi Hping3 dengan metode SYN Flood untuk menghasilkan lonjakan trafik secara signifikan.

Parameter yang diukur dalam penelitian ini meliputi throughput, delay, dan packet loss sebagai indikator *Quality of Service* (QoS). Selain itu, dilakukan monitoring terhadap penggunaan CPU pada router MikroTik untuk mengetahui dampak serangan terhadap performa sistem. Data hasil pengujian kemudian dianalisis untuk mengevaluasi efektivitas implementasi firewall dalam memitigasi serangan DDoS serta menjaga stabilitas jaringan.

3.3 Alat dan Bahan

Berdasarkan hasil identifikasi kebutuhan penelitian, perangkat yang digunakan diklasifikasikan menjadi dua kategori utama, yaitu perangkat keras dan perangkat lunak. Perangkat keras digunakan untuk membangun serta menjalankan sistem jaringan yang diuji, sedangkan perangkat lunak digunakan untuk mendukung proses konfigurasi, simulasi serangan, serta analisis performa jaringan.

Perangkat keras dalam penelitian ini terdiri dari router MikroTik yang berfungsi sebagai pusat pengelola jaringan, komputer client yang digunakan untuk melakukan monitoring jaringan, komputer attacker yang digunakan untuk mensimulasikan serangan DDoS, serta perangkat switch sebagai penghubung antar jaringan. Spesifikasi perangkat keras yang digunakan dalam penelitian ini disajikan pada Tabel 2.

Tabel 2 Perangkat keras yang digunakan

No	Jenis Perangkat	Spesifikasi	Keterangan
1	Router MikroTik	RB750Gr3, CPU 880 MHz, RAM 256 MB	Pengelola jaringan
2	Komputer Client	Intel Core i5, RAM 8 GB	Monitoring jaringan
3	Komputer Attacker	Intel Core i5, RAM 8 GB	Simulasi serangan
4	Switch	TP-Link 8 Port Gigabit	Penghubung jaringan

Sementara itu, perangkat lunak yang digunakan meliputi MikroTik RouterOS sebagai sistem operasi pada router, Winbox sebagai alat konfigurasi, Kali Linux sebagai sistem operasi untuk simulasi serangan, Hping3 sebagai tools untuk melakukan pengujian serangan DDoS, serta Wireshark untuk melakukan analisis lalu lintas jaringan. Daftar perangkat lunak yang digunakan ditunjukkan pada Tabel 3.

Tabel 3 Perangkat lunak yang digunakan

No	Jenis Perangkat	Versi	Keterangan
1	MikroTik RouterOS	6.49.18 (Long-term)	Sistem operasi pada router MikroTik.
2	Winbox	3.40	Aplikasi konfigurasi router MikroTik.
3	Kali Linux	2023.4	Sistem operasi untuk simulasi serangan.
4	Hping3	3.0.0-alpha-2	Tools simulasi serangan DDoS.
5	Wireshark	4.2.5	Tools analisis lalu lintas jaringan.

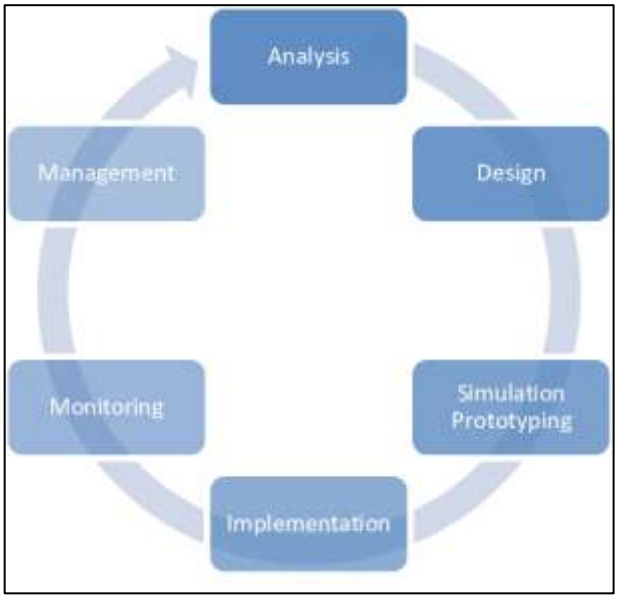
Pemilihan perangkat keras dan perangkat lunak dalam penelitian ini didasarkan pada pertimbangan kestabilan sistem serta kesesuaian dengan kebutuhan pengujian, sehingga hasil yang diperoleh dapat menggambarkan kondisi jaringan secara nyata dan dapat direplikasi pada lingkungan yang serupa.

 ISSN:2302-8149
e-ISSN:2540-9719

3.4 Metode Network Development Life Cycle (NDLC)

Metode yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC), yaitu pendekatan sistematis dalam pengembangan jaringan komputer yang mencakup beberapa tahapan terstruktur mulai dari perencanaan hingga evaluasi sistem [9]. Metode ini dipilih karena mampu memberikan alur kerja yang jelas dalam merancang, mengimplementasikan, serta menganalisis performa jaringan secara menyeluruh.

NDLC terdiri dari beberapa tahapan utama yang saling berkaitan, yaitu analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Setiap tahapan memiliki peran penting dalam memastikan bahwa sistem jaringan yang dibangun dapat berjalan sesuai dengan kebutuhan serta mampu menghadapi potensi gangguan yang mungkin terjadi.



Gambar 2 Metode NDLC

Berdasarkan Gambar 2 proses NDLC dimulai dari tahap analisis, yaitu mengidentifikasi kebutuhan jaringan serta permasalahan yang ada. Pada penelitian ini, proses analisis dilakukan dengan mengamati kondisi jaringan di Diskominfo Kota Kediri yang belum memiliki sistem firewall sebagai mekanisme pengamanan, sehingga berpotensi mengalami gangguan akibat trafik yang tidak normal.
Selanjutnya, tahap desain dilakukan untuk merancang sistem jaringan yang akan diterapkan. Proses ini mencakup perancangan topologi jaringan serta konfigurasi firewall, termasuk penentuan aturan filtering, pembatasan koneksi, dan mekanisme pencegahan serangan DDoS.

Setelah desain selesai, dilakukan tahap simulasi untuk menguji rancangan sebelum diimplementasikan secara langsung. Dalam penelitian ini, simulasi dilakukan dengan melakukan pengujian serangan DDoS pada lingkungan jaringan uji coba guna melihat respons sistem terhadap lonjakan trafik.

Tahap berikutnya adalah implementasi, yaitu proses penerapan desain yang telah dibuat ke dalam perangkat nyata. Implementasi dilakukan dengan mengkonfigurasi firewall pada router MikroTik sesuai dengan aturan yang telah ditentukan sebelumnya.

Setelah sistem berjalan, dilakukan tahap monitoring untuk mengamati aktivitas jaringan serta mengevaluasi performa sistem dalam menangani trafik yang masuk. Proses ini bertujuan untuk mengetahui efektivitas firewall dalam menjaga stabilitas jaringan selama pengujian berlangsung.

Tahap terakhir adalah manajemen, yang mencakup proses evaluasi dan pengelolaan sistem secara keseluruhan. Pada tahap ini dilakukan analisis terhadap hasil pengujian serta penyesuaian konfigurasi jika diperlukan, sehingga sistem dapat berjalan lebih optimal dan berkelanjutan.

Dengan menggunakan metode NDLC, proses pengembangan jaringan dalam penelitian ini dapat dilakukan secara terstruktur dan sistematis, sehingga hasil yang diperoleh lebih mudah dianalisis serta dapat memberikan gambaran yang jelas mengenai efektivitas implementasi firewall dalam meningkatkan keamanan jaringan.

 ISSN:2302-8149
e-ISSN:2540-9719

3.5 Parameter Pengujian

Parameter pengujian dalam penelitian ini digunakan untuk mengevaluasi performa jaringan sebelum dan sesudah implementasi firewall MikroTik. Pengujian dilakukan dengan mengamati perubahan kualitas layanan jaringan akibat adanya perlakuan berupa penerapan mekanisme keamanan.

Parameter utama yang digunakan mengacu pada indikator *Quality of Service* (QoS), yaitu throughput, delay, dan packet loss. Parameter-parameter ini dipilih karena secara umum digunakan dalam analisis performa jaringan dan mampu memberikan gambaran kuantitatif terhadap kondisi jaringan yang diuji.

Throughput digunakan untuk mengukur kemampuan jaringan dalam mentransmisikan data dalam satuan waktu tertentu. Parameter ini menunjukkan kapasitas jaringan dalam menangani trafik, baik pada kondisi normal maupun saat terjadi serangan.

Delay atau latensi digunakan untuk mengukur waktu yang dibutuhkan oleh paket data untuk mencapai tujuan. Nilai delay yang rendah menunjukkan bahwa jaringan mampu merespon dengan cepat, sedangkan peningkatan delay umumnya terjadi akibat adanya gangguan atau beban trafik yang tinggi.

Packet loss digunakan untuk mengukur persentase paket data yang hilang selama proses transmisi. Parameter ini menjadi indikator penting dalam menilai stabilitas jaringan, karena semakin tinggi nilai packet loss maka kualitas komunikasi data akan semakin menurun.

Berdasarkan standar *Quality of Service* (QoS), performa jaringan dapat dievaluasi melalui ketiga parameter tersebut yang mencerminkan kemampuan transmisi data, waktu tunda pengiriman, serta tingkat kehilangan paket [22].

Selain parameter QoS, penelitian ini juga menggunakan penggunaan CPU pada router MikroTik sebagai parameter pendukung untuk mengamati beban kerja sistem selama proses pengujian. Penggunaan CPU tidak termasuk dalam parameter QoS, namun digunakan sebagai indikator performa perangkat dalam menangani trafik jaringan. Dalam sistem jaringan modern, penggunaan CPU berkaitan erat dengan kemampuan perangkat dalam memproses paket data, di mana peningkatan beban trafik dapat menyebabkan CPU menjadi bottleneck yang berdampak pada penurunan performa jaringan [23]. Penelitian lain juga menunjukkan bahwa tingkat utilisasi CPU memiliki hubungan langsung dengan kemampuan transfer data dalam jaringan [24].

Nilai CPU yang mendekati 100% menunjukkan bahwa perangkat mengalami beban kerja yang sangat tinggi, sedangkan nilai CPU yang rendah menunjukkan kondisi sistem yang stabil dan mampu menangani trafik secara optimal. Dengan demikian, parameter CPU digunakan untuk memperkuat analisis terhadap dampak serangan DDoS serta efektivitas firewall dalam mengurangi beban sistem.

4. Hasil dan Pembahasan

Bagian ini menyajikan hasil penelitian berdasarkan tahapan metode Network Development Life Cycle (NDLC) yang telah dilakukan. Setiap tahapan menghasilkan data dan temuan yang digunakan untuk mengevaluasi efektivitas firewall MikroTik dalam mencegah serangan Distributed Denial of Service (DDoS).

4.1 Hasil Analisis

Tahap analisis merupakan tahap awal dalam penelitian yang bertujuan untuk mengidentifikasi kondisi jaringan eksisting serta permasalahan yang terjadi pada jaringan di Diskominfo Kota Kediri. Analisis dilakukan melalui metode observasi langsung terhadap infrastruktur jaringan yang sedang berjalan.

Berdasarkan hasil analisis, jaringan yang digunakan memiliki topologi terpusat dengan satu router MikroTik yang terhubung ke internet melalui ISP. Router MikroTik berfungsi sebagai pusat pengendali jaringan yang mendistribusikan koneksi ke beberapa segmen jaringan pada masing-masing bagian, yaitu Sekretariat, Ruang IKPTIK, Ruang TKSDPIP, dan Ruang APTIKA. Setiap segmen jaringan terhubung melalui switch dan menyediakan akses bagi perangkat client serta access point.

Kondisi ini menunjukkan bahwa router MikroTik memiliki peran yang sangat krusial sebagai titik sentral dalam pengelolaan dan pengamanan jaringan, sehingga apabila tidak dilengkapi dengan

 ISSN:2302-8149
e-ISSN:2540-9719

sistem keamanan yang memadai, maka seluruh jaringan berpotensi terdampak secara langsung oleh serangan.

Berdasarkan topologi jaringan yang telah dirancang pada Gambar 1, seluruh trafik jaringan internal akan melewati router MikroTik sebelum menuju jaringan eksternal (internet). Kondisi ini menjadikan router MikroTik sebagai titik sentral dalam pengelolaan serta pengamanan jaringan, sehingga implementasi firewall difokuskan pada perangkat tersebut untuk mengontrol dan memfilter lalu lintas data yang masuk maupun keluar jaringan.

Selain topologi jaringan, analisis juga dilakukan terhadap alokasi alamat IP yang digunakan pada masing-masing segmen jaringan. Skema pengalamatan IP yang digunakan pada penelitian ini mengikuti rancangan jaringan yang telah dijelaskan pada Tabel 1. Penggunaan segmentasi IP yang terstruktur memudahkan proses pengelolaan jaringan serta penerapan mekanisme filtering pada router MikroTik.

Berdasarkan Tabel 1, alokasi alamat IP menggunakan skema subnetting jaringan privat untuk masing-masing segmen yang terhubung ke router MikroTik sebagai gateway utama. Koneksi ke jaringan eksternal menggunakan IP publik dari ISP dengan subnet /29, sehingga seluruh trafik jaringan lokal akan melewati router MikroTik sebelum menuju ke internet. Kondisi ini memungkinkan penerapan sistem keamanan jaringan secara terpusat.

Namun, sistem keamanan jaringan yang diterapkan masih belum optimal. Router MikroTik belum dikonfigurasi sebagai firewall secara maksimal, sehingga belum terdapat mekanisme filtering trafik maupun pembatasan koneksi yang memadai. Hal ini menyebabkan jaringan rentan terhadap serangan Distributed Denial of Service (DDoS) yang dapat mengganggu ketersediaan layanan.

Berdasarkan permasalahan tersebut, diperlukan sistem keamanan jaringan yang mampu memfilter trafik, membatasi koneksi mencurigakan, serta mengurangi dampak serangan DDoS. Selain itu, dilakukan pengujian dengan mensimulasikan serangan DDoS untuk membandingkan performa jaringan sebelum dan sesudah implementasi firewall menggunakan parameter throughput, delay, dan packet loss.

Hasil dari tahap analisis ini menjadi dasar dalam perancangan dan implementasi firewall MikroTik pada tahap selanjutnya.

4.2 Hasil Desain

Tahap desain merupakan tahap perancangan sistem keamanan jaringan berdasarkan hasil analisis yang telah dilakukan sebelumnya. Pada tahap ini difokuskan pada perancangan mekanisme firewall pada router MikroTik untuk mencegah serangan Distributed Denial of Service (DDoS).

Berdasarkan topologi jaringan yang digunakan, seluruh trafik dari jaringan internal menuju jaringan eksternal akan melewati router MikroTik. Oleh karena itu, router dikonfigurasi sebagai pusat pengendali keamanan jaringan dengan menerapkan aturan firewall (*firewall rules*) yang berfungsi untuk mengontrol, memfilter, dan membatasi lalu lintas data.

Perancangan firewall dilakukan dengan pendekatan filtering berbasis koneksi dan perilaku trafik. Sistem dirancang untuk mampu mendeteksi trafik yang tidak normal, seperti lonjakan koneksi dalam jumlah besar dari satu sumber, yang merupakan karakteristik serangan DDoS.

Secara umum, mekanisme firewall yang dirancang meliputi:

a. Penyaringan paket data berdasarkan status koneksi (*connection state*)
b. Pembatasan jumlah koneksi dari satu alamat IP
c. Identifikasi dan pemblokiran IP yang mencurigakan
d. Pembuangan paket data yang tidak valid (*invalid packet*)

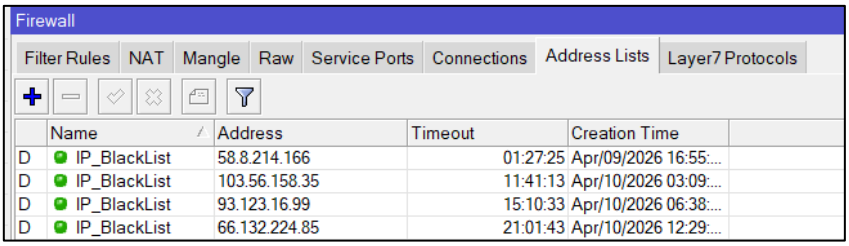
 ISSN:2302-8149
e-ISSN:2540-9719

```
/ip firewall filter
# Fungsi: Mengizinkan paket yang sudah terverifikasi agar tidak diproses berulang oleh CPU.
add action=accept chain=input connection-state=established,related,untracked comment="ACCEPT: Koneksi input yang sudah terjalin/aman"
add action=accept chain=forward connection-state=established,related,untracked comment="ACCEPT: Koneksi forward yang sudah terjalin/aman"

# Fungsi: Membuang paket yang tidak memiliki status jelas sebelum membebani sistem lebih jauh.
add action=drop chain=input connection-state=invalid comment="DROP: Paket input tidak valid"
add action=drop chain=forward connection-state=invalid comment="DROP: Paket forward tidak valid"

# Fungsi: Mengalihkan trafik baru (new) ke rantai (chain) khusus 'detect-ddos' untuk dianalisa.
add action=jump chain=input connection-state=new jump-target=detect-ddos comment="DDOS: Lempar trafik input baru ke deteksi"
add action=jump chain=forward connection-state=new jump-target=detect-ddos comment="DDOS: Lempar trafik forward baru ke deteksi"

# Fungsi: Jika trafik di bawah limit (32 koneksi/10 detik), kembalikan ke proses normal.
# Jika di atas limit, maka aturan di bawahnya akan mencatat IP tersebut sebagai penyerang.
add action=return chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s comment="DDOS: Normal jika di bawah limit (kembali ke filter)"

# Aturan ini hanya tercapai jika limit di atas terlampaui (terdeteksi serangan):
add action=add-dst-to-address-list address-list=ddos-targets address-list-timeout=10m chain=detect-ddos comment="DDOS: Catat IP Target"
add action=add-src-to-address-list address-list=ddos-attackers address-list-timeout=10m chain=detect-ddos comment="DDOS: Catat IP Attacker"
/ip firewall raw
# Fungsi: Membuang paket dari penyerang ke korban SEBELUM masuk ke Connection Tracking.
add action=drop chain=prerouting src-address-list=ddos-attackers dst-address-list=ddos-targets comment="RAW: Blokir serangan DDoS secara efisien"
```

Gambar 3 Konfigurasi firewall filter rules pada MikroTik

Berdasarkan Gambar 3 konfigurasi firewall pada router MikroTik terdiri dari beberapa aturan utama yang digunakan untuk mengontrol lalu lintas jaringan. Aturan *accept established* dan *related* digunakan untuk mengizinkan koneksi yang telah terbentuk agar komunikasi jaringan tetap berjalan dengan normal.

Selanjutnya, aturan *drop invalid* digunakan untuk membuang paket data yang tidak valid, sehingga dapat mengurangi beban sistem akibat trafik yang tidak normal. Selain itu, terdapat aturan khusus untuk mendeteksi pola serangan DDoS melalui mekanisme pembatasan koneksi dan identifikasi trafik mencurigakan.



Gambar 4 Address list (blacklist) pada MikroTik

Pada Gambar 4 ditunjukkan penggunaan fitur *address list* yang berfungsi sebagai daftar blokir (*blacklist*). Alamat IP yang terdeteksi melakukan aktivitas mencurigakan secara otomatis dimasukkan ke dalam daftar tersebut dan akan diblokir oleh sistem. Mekanisme ini memungkinkan sistem untuk mencegah akses berulang dari sumber serangan.

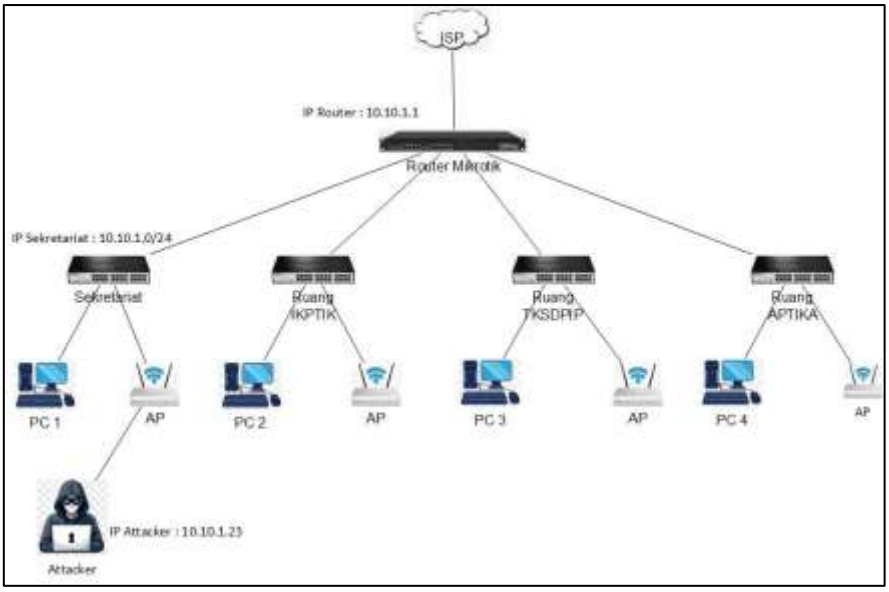
Dengan konfigurasi tersebut, firewall MikroTik mampu melakukan filtering trafik secara efektif serta mengurangi potensi serangan Distributed Denial of Service (DDoS) pada jaringan. Perancangan ini menjadi dasar dalam membangun sistem keamanan yang mampu mendeteksi dan membatasi trafik tidak normal sebelum berdampak pada jaringan secara keseluruhan.

4.3 Hasil Simulasi

Pada tahap simulasi, dilakukan pengujian dengan mensimulasikan serangan Distributed Denial of Service (DDoS) untuk mengetahui respon jaringan terhadap trafik dalam jumlah besar. Simulasi dilakukan menggunakan aplikasi Hping3 dengan metode SYN Flood yang dijalankan dari perangkat attacker dengan alamat IP 10.10.1.23 menuju router MikroTik sebagai gateway utama dengan IP 10.10.1.1. Seluruh trafik serangan melewati router sebelum didistribusikan ke beberapa segmen jaringan, yaitu Sekretariat, IKPTIK, TKSDPIP, dan APTIKA.

Alur simulasi serangan DDoS pada penelitian ini ditunjukkan pada Gambar 5.

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 5 Topologi simulasi serangan DDoS

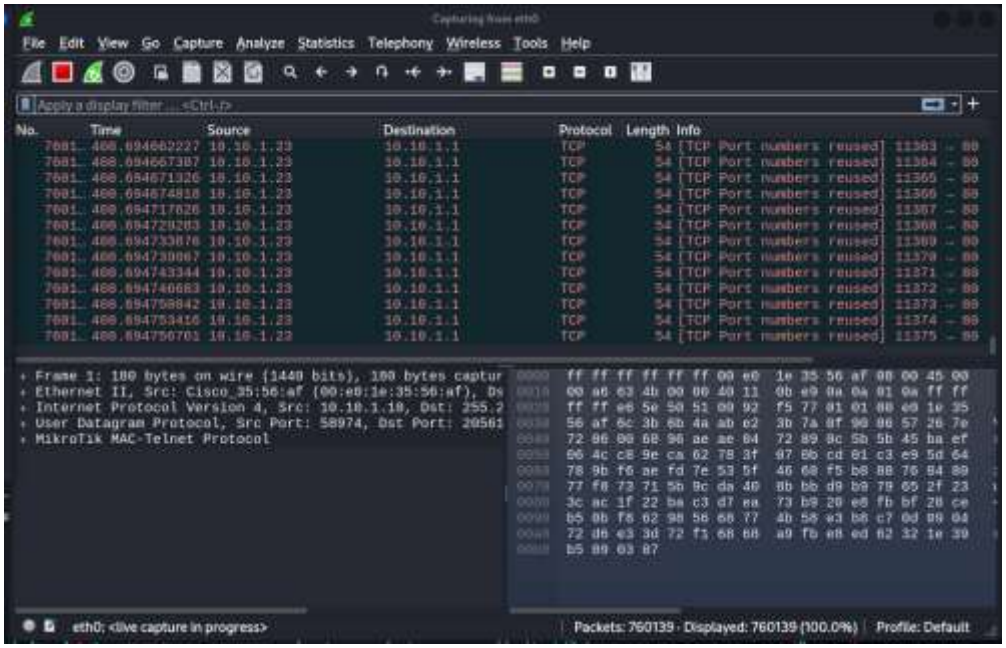
Berdasarkan Gambar 5 proses simulasi dimulai dari attacker yang mengirimkan paket SYN secara terus-menerus menuju router MikroTik. Pada kondisi sebelum firewall diterapkan, seluruh trafik serangan diteruskan langsung ke jaringan internal tanpa adanya proses penyaringan, sehingga menyebabkan peningkatan beban jaringan. Sebaliknya, pada kondisi setelah firewall diaktifkan, trafik yang mencurigakan akan difilter dan dibatasi sebelum diteruskan ke jaringan internal, sehingga dampak serangan dapat dikurangi.

Untuk membuktikan bahwa serangan berhasil dilakukan, digunakan terminal Hping3 sebagai penghasil trafik serangan dan Wireshark sebagai alat untuk menganalisis paket yang masuk ke jaringan.

Gambar 6 Simulasi serangan menggunakan hping3

Berdasarkan Gambar 6 terlihat bahwa perintah *hping3 -S --flood -p 80 10.10.1.1* digunakan untuk mengirimkan paket SYN secara terus-menerus menuju target. Mode *flood* menyebabkan paket dikirim tanpa henti sehingga menghasilkan lonjakan trafik dalam waktu singkat. Hasil pengujian menunjukkan bahwa serangan DDoS berhasil disimulasikan dan menghasilkan trafik dalam jumlah besar.

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 7 Hasil capture trafik menggunakan wireshark

Berdasarkan Gambar 7 terlihat bahwa Wireshark menangkap sejumlah besar paket TCP yang dikirim secara berulang dari alamat IP 10.10.1.23 menuju 10.10.1.1. Banyaknya paket dengan pola yang sama dalam waktu yang sangat singkat menunjukkan karakteristik serangan SYN Flood. Trafik yang dihasilkan terlihat sangat padat dan berulang, yang mengindikasikan adanya aktivitas serangan DDoS pada jaringan.

Pada kondisi tanpa firewall, seluruh paket tersebut diteruskan ke jaringan internal tanpa adanya pembatasan, sehingga menyebabkan trafik menjadi tidak terkendali dan berpotensi mengganggu kinerja jaringan. Sedangkan setelah firewall diterapkan, sebagian trafik yang mencurigakan mulai difilter dan dibatasi, sehingga jumlah paket yang masuk ke jaringan menjadi lebih terkendali.

Hasil simulasi ini menunjukkan bahwa serangan DDoS dapat diidentifikasi melalui lonjakan trafik yang signifikan dan pola paket yang berulang, serta membuktikan bahwa firewall MikroTik mampu merespon serangan dengan melakukan filtering terhadap trafik yang tidak normal sebelum memasuki jaringan internal. Perbedaan kondisi sebelum dan sesudah penerapan firewall akan dianalisis lebih lanjut pada tahap monitoring.

Hal ini menegaskan bahwa tanpa mekanisme filtering, jaringan tidak memiliki kemampuan untuk membedakan trafik normal dan trafik serangan, sehingga seluruh paket akan diproses secara bersamaan dan berpotensi menyebabkan penurunan performa.

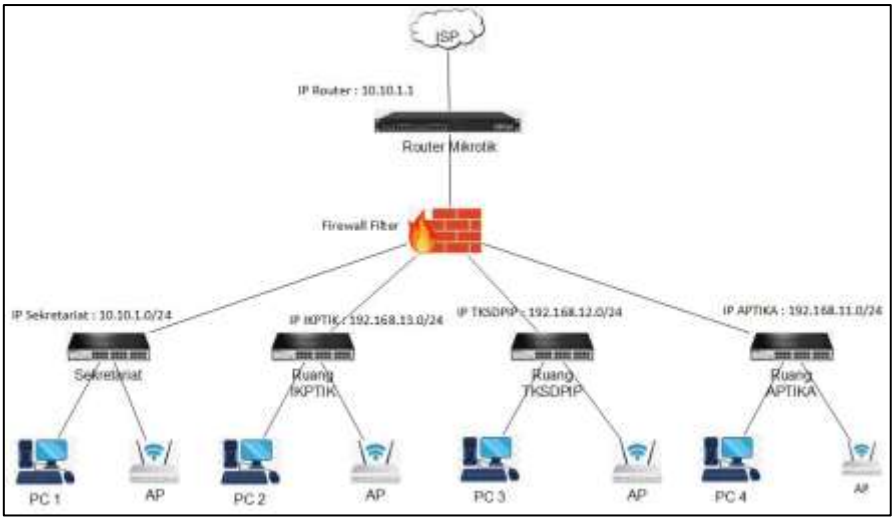
4.4 Hasil Implementasi

Pada tahap implementasi, dilakukan penerapan sistem firewall pada router MikroTik berdasarkan rancangan yang telah dibuat pada tahap sebelumnya. Implementasi ini bertujuan untuk mengontrol lalu lintas jaringan serta membatasi koneksi yang mencurigakan guna mencegah terjadinya serangan Distributed Denial of Service (DDoS).

Firewall diimplementasikan pada router MikroTik sebagai gateway utama yang menghubungkan jaringan internal dengan jaringan eksternal. Dengan posisi tersebut, seluruh trafik yang masuk dan keluar jaringan akan melewati proses penyaringan sebelum diteruskan ke masing-masing segmen jaringan.

Hasil implementasi firewall pada topologi jaringan ditunjukkan pada Gambar 8.

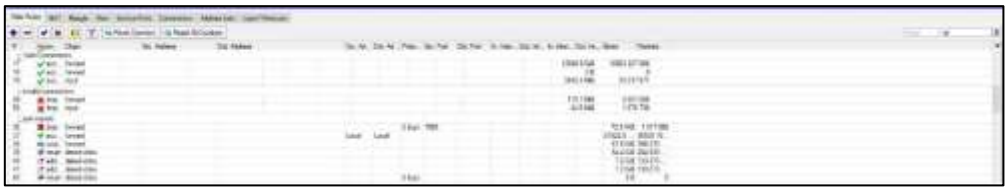
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 8 Implementasi firewall pada jaringan

Berdasarkan Gambar 8 firewall ditempatkan pada router MikroTik sebagai pusat pengendali jaringan. Seluruh trafik dari jaringan eksternal maupun internal akan melewati firewall sebelum didistribusikan ke segmen jaringan seperti Sekretariat, IKPTIK, TKSDPIP, dan APTIKA. Dengan demikian, firewall berfungsi sebagai mekanisme kontrol utama dalam menyaring paket data yang masuk ke dalam jaringan.

Selain itu, konfigurasi firewall yang telah diterapkan pada router MikroTik ditunjukkan pada Gambar 9.



Gambar 9 Konfigurasi firewall mikrotik

Berdasarkan Gambar 9 terlihat bahwa aturan firewall telah diimplementasikan dan berjalan pada router MikroTik. Hal ini ditunjukkan dengan adanya nilai pada kolom *bytes* dan *packets*, yang menandakan bahwa aturan firewall telah memproses lalu lintas jaringan secara aktif.

Aturan yang diterapkan meliputi *accept established* dan *related* untuk menjaga koneksi yang valid tetap berjalan, serta *drop invalid* untuk membuang paket yang tidak valid. Selain itu, terdapat mekanisme pembatasan koneksi dan deteksi trafik mencurigakan yang digunakan untuk mengidentifikasi pola serangan DDoS.

Dengan konfigurasi tersebut, firewall mampu melakukan penyaringan terhadap trafik yang tidak normal serta membatasi koneksi yang berpotensi mengganggu kestabilan jaringan. Kondisi ini mengindikasikan bahwa sistem keamanan yang diimplementasikan telah berjalan sesuai dengan rancangan yang telah dibuat sebelumnya.

Secara keseluruhan, hasil implementasi menunjukkan bahwa firewall MikroTik dapat berfungsi sebagai sistem proteksi jaringan yang efektif, serta mampu mengontrol lalu lintas data secara terpusat sebelum dilakukan pengujian lebih lanjut pada tahap monitoring.

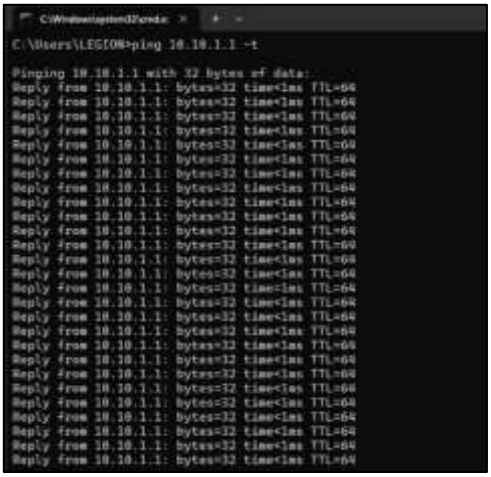
4.5 Hasil Monitoring

Pada tahap monitoring, dilakukan pengamatan terhadap performa jaringan untuk mengetahui dampak serangan Distributed Denial of Service (DDoS) serta efektivitas firewall dalam mengendalikan trafik jaringan. Pengamatan dilakukan dengan membandingkan tiga kondisi, yaitu kondisi normal, kondisi saat serangan DDoS tanpa firewall, dan kondisi saat serangan DDoS dengan firewall aktif.

Parameter yang digunakan dalam pengujian meliputi throughput, delay, packet loss, dan penggunaan CPU pada router MikroTik. Pengukuran delay dan packet loss dilakukan menggunakan perintah *ping*, sedangkan throughput diamati melalui fitur monitoring trafik pada

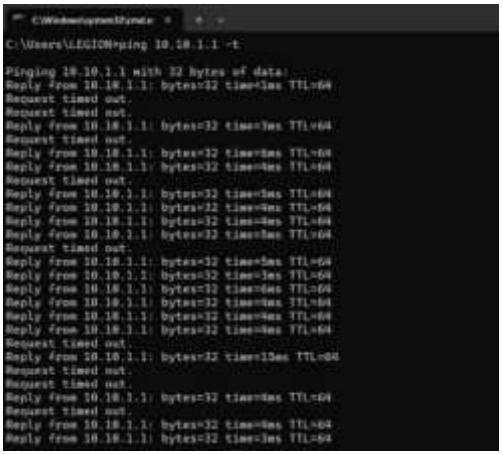
 ISSN:2302-8149
e-ISSN:2540-9719

router MikroTik.



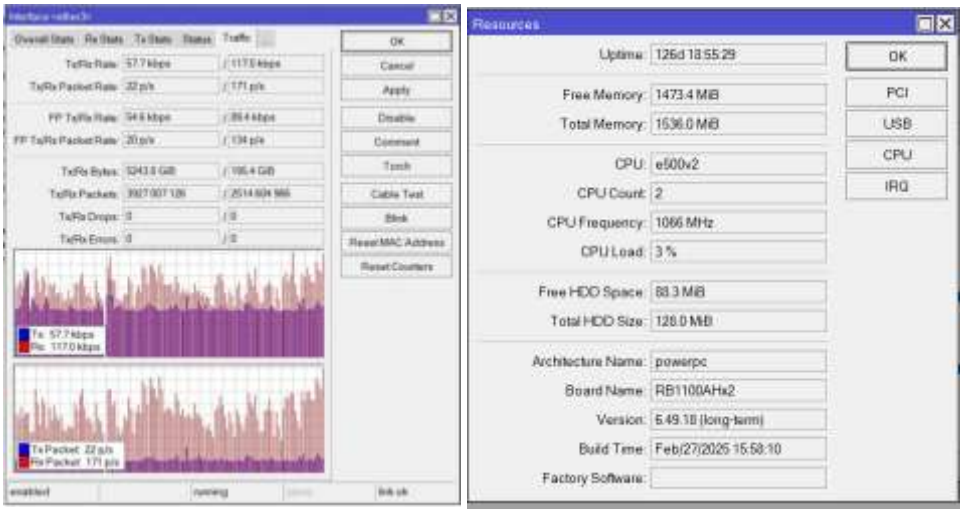
Gambar 10 Kondisi jaringan normal (ping)

Berdasarkan Gambar 10 terlihat bahwa kondisi jaringan pada saat normal menunjukkan waktu respon yang stabil dengan nilai delay kurang dari 1 ms serta tidak terdapat *request timed out*. Hasil pengujian menunjukkan bahwa tidak terjadi packet loss dan jaringan berada dalam kondisi optimal.



Gambar 11 Kondisi jaringan saat serangan (ping)

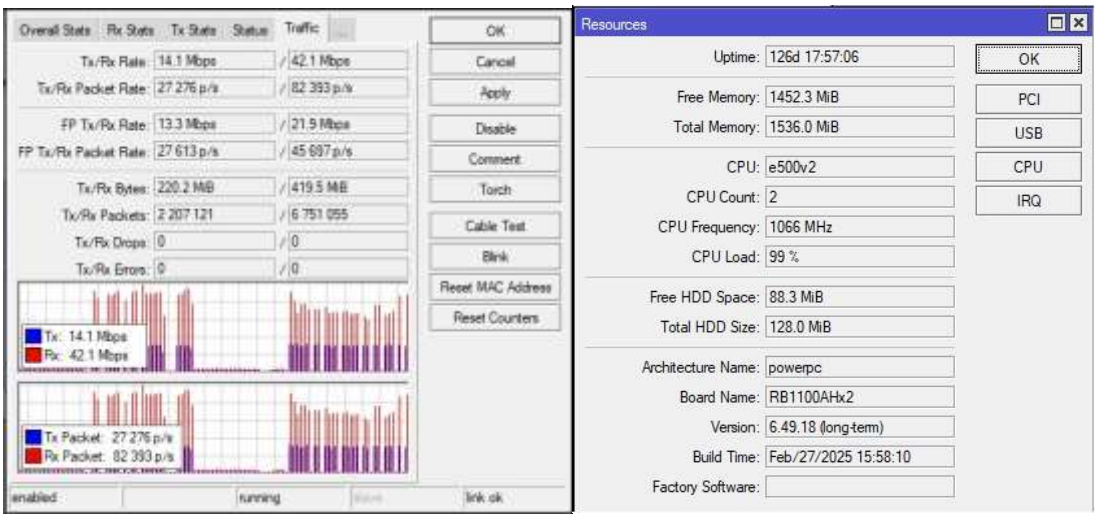
Berdasarkan Gambar 11 terlihat adanya beberapa *request timed out* serta fluktuasi nilai delay yang meningkat hingga lebih dari 5 ms. Kondisi ini menunjukkan terjadinya packet loss dan penurunan kualitas jaringan akibat serangan DDoS.



Gambar 12 Trafik jaringan saat normal + penggunaan CPU

 ISSN:2302-8149
e-ISSN:2540-9719

Berdasarkan Gambar 12 terlihat bahwa trafik jaringan pada kondisi normal relatif stabil dengan nilai throughput yang rendah, yaitu sekitar ±0.1 Mbps untuk Tx dan ±0.1 Mbps untuk Rx. Hal ini menunjukkan bahwa tidak terdapat aktivitas trafik yang berlebihan pada jaringan. Pada kondisi normal, penggunaan CPU pada router MikroTik berada pada kisaran 3%, seperti yang ditunjukkan pada Gambar 12. Hasil pengujian menunjukkan bahwa sistem berjalan dalam kondisi stabil dengan beban kerja yang rendah.



Gambar 13 Trafik jaringan saat serangan + penggunaan CPU

Berdasarkan Gambar 13 terlihat adanya lonjakan trafik yang signifikan dengan throughput mencapai lebih dari 40 Mbps serta peningkatan jumlah paket per detik yang tinggi. Hasil pengujian menunjukkan adanya trafik dalam jumlah besar yang dikirim secara terus-menerus oleh attacker, sehingga menyebabkan beban jaringan meningkat secara drastis.

Selain peningkatan trafik, serangan DDoS juga berdampak signifikan terhadap penggunaan sumber daya router. Berdasarkan Gambar 13, terlihat bahwa penggunaan CPU pada router MikroTik meningkat hingga mencapai 99%-100% saat serangan berlangsung. Kondisi ini menunjukkan bahwa router mengalami beban kerja yang sangat tinggi akibat banyaknya paket yang masuk secara bersamaan.

Tingginya penggunaan CPU ini menyebabkan penurunan performa jaringan, yang ditandai dengan meningkatnya delay serta munculnya packet loss pada pengujian sebelumnya. Kondisi ini mengindikasikan bahwa tanpa adanya mekanisme filtering, sistem tidak mampu menangani trafik serangan secara optimal.

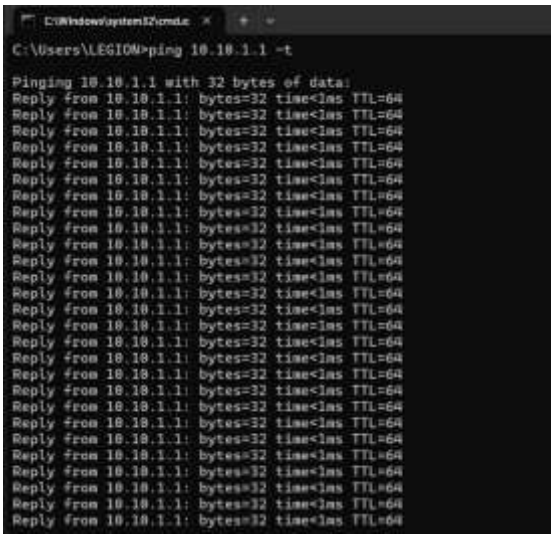
Hasil pengujian menunjukkan bahwa pada kondisi serangan DDoS tanpa firewall, penggunaan CPU meningkat hingga mencapai 100% sehingga menyebabkan penurunan performa jaringan secara signifikan. Setelah firewall diimplementasikan, penggunaan CPU kembali stabil dan berada pada kisaran rendah. Kondisi ini menunjukkan bahwa firewall mampu mengurangi beban sistem akibat serangan.

 ISSN:2302-8149
e-ISSN:2540-9719

Gambar 14 Trafik jaringan saat serangan + firewall aktif (penggunaan CPU)

Berdasarkan Gambar 14 kondisi serangan DDoS dengan firewall aktif, terlihat bahwa trafik jaringan masih mengalami peningkatan, namun tidak sebesar kondisi tanpa firewall. Nilai throughput berada pada kisaran sekitar 2 Mbps pada sisi penerimaan (Rx), yang menunjukkan bahwa sebagian besar trafik serangan telah berhasil difilter oleh firewall.

Selain itu, penggunaan CPU pada router MikroTik tetap berada pada kondisi rendah, yaitu sekitar 3%, yang menunjukkan bahwa sistem tidak mengalami beban berlebih karena mekanisme filtering berjalan dengan baik.



Gambar 15 Kondisi jaringan saat DDoS dengan firewall aktif (ping)

Berdasarkan Gambar 15 kondisi serangan DDoS dengan firewall aktif, hasil pengujian menggunakan perintah *ping* menunjukkan bahwa jaringan tetap stabil dengan waktu respon kurang dari 1 ms serta tidak ditemukan *request timed out*. Hasil pengujian menunjukkan bahwa firewall mampu memfilter trafik serangan secara efektif sehingga tidak mempengaruhi kualitas koneksi jaringan.

Kondisi ini menunjukkan bahwa firewall tidak hanya mampu memfilter trafik berbahaya, tetapi juga berperan dalam menjaga kestabilan jaringan dengan mengurangi beban kerja pada perangkat router. Dengan demikian, sistem tetap mampu melayani trafik normal meskipun terjadi serangan.

Tabel 4 Perbandingan kualitas jaringan

Parameter	Normal	DDoS Tanpa Firewall	DDoS + Firewall
Throughput	±0.1 Mbps	±40 Mbps	±2 Mbps

 ISSN:2302-8149
e-ISSN:2540-9719

Delay	<1 ms	5–15 ms	<1 ms
Packet Loss	0%	±20–30%	0%
CPU Usage	3%	99–100%	±3%

Berdasarkan Tabel 4 terlihat bahwa serangan DDoS memberikan dampak yang signifikan terhadap kualitas jaringan. Pada kondisi normal, jaringan menunjukkan performa yang stabil dengan nilai throughput rendah, delay yang sangat kecil, serta tidak adanya packet loss.

Perbedaan yang signifikan antara ketiga kondisi tersebut menunjukkan bahwa firewall MikroTik memiliki peran yang sangat penting dalam menjaga kualitas layanan jaringan. Tanpa firewall, jaringan mengalami overload akibat trafik berlebih, sedangkan dengan firewall, sistem mampu mengontrol trafik sehingga performa jaringan tetap stabil. Hal ini membuktikan bahwa implementasi firewall efektif dalam memitigasi serangan DDoS secara langsung.

Sebaliknya, pada saat terjadi serangan DDoS, terjadi peningkatan throughput secara drastis akibat masuknya trafik dalam jumlah besar. Hal ini diikuti dengan meningkatnya delay serta munculnya packet loss yang cukup signifikan, yang mengindikasikan bahwa jaringan mengalami overload.

Setelah penerapan firewall MikroTik, sistem mampu mengontrol trafik yang masuk dengan lebih baik melalui mekanisme filtering. Trafik yang mencurigakan tidak seluruhnya diteruskan ke jaringan internal, sehingga beban jaringan dapat dikurangi dan kestabilan jaringan tetap terjaga.

Dengan demikian, hasil monitoring menunjukkan bahwa implementasi firewall MikroTik efektif dalam meningkatkan kualitas jaringan serta mengurangi dampak serangan DDoS berdasarkan parameter throughput, delay, dan packet loss.

Hasil penelitian ini sejalan dengan beberapa penelitian sebelumnya yang menunjukkan bahwa implementasi firewall MikroTik mampu meningkatkan keamanan serta performa jaringan. Penelitian [10] menunjukkan bahwa mekanisme filtering pada firewall efektif dalam mengurangi dampak serangan DoS dengan cara membatasi trafik yang tidak normal. Selain itu, penelitian [12] dan [13] juga menyatakan bahwa konfigurasi firewall yang tepat dapat meningkatkan kontrol terhadap lalu lintas jaringan serta memberikan fleksibilitas dalam pengelolaan trafik.

Temuan dalam penelitian ini juga konsisten dengan hasil penelitian [14] dan [15] yang menunjukkan bahwa penerapan sistem keamanan berbasis firewall mampu meningkatkan stabilitas jaringan serta mengurangi gangguan layanan akibat lonjakan trafik. Lebih lanjut, penelitian [16] dan [17] menegaskan bahwa firewall MikroTik efektif digunakan dalam berbagai lingkungan, termasuk instansi pemerintahan, dalam menjaga kualitas layanan jaringan.

Perbedaan utama penelitian ini dibandingkan penelitian sebelumnya terletak pada pendekatan pengujian yang dilakukan secara komparatif dalam tiga kondisi, yaitu kondisi normal, saat serangan DDoS, dan setelah penerapan firewall. Hasil yang diperoleh menunjukkan bahwa firewall tidak hanya berfungsi sebagai mekanisme keamanan, tetapi juga berperan dalam menjaga performa jaringan dengan menurunkan beban CPU serta mempertahankan stabilitas parameter QoS.

4.6 Hasil Manajemen

Pada tahap manajemen, dilakukan pengelolaan terhadap sistem keamanan jaringan yang telah diimplementasikan untuk memastikan bahwa firewall MikroTik dapat berjalan secara optimal dan berkelanjutan. Tahap ini mencakup pengaturan kebijakan keamanan, pemeliharaan sistem, serta evaluasi terhadap kinerja firewall dalam menghadapi potensi serangan.

Pengelolaan sistem dilakukan dengan memastikan bahwa konfigurasi firewall tetap berjalan sesuai dengan aturan yang telah ditetapkan. Administrator jaringan melakukan pengecekan secara berkala terhadap aturan firewall, terutama pada bagian *filter rules* dan *address list*, untuk memastikan bahwa tidak terdapat konfigurasi yang tidak sesuai atau berpotensi menimbulkan celah keamanan.

Selain itu, dilakukan pengelolaan terhadap daftar alamat IP yang terindikasi sebagai sumber serangan dengan memanfaatkan fitur *address list* pada MikroTik. Alamat IP yang terdeteksi melakukan aktivitas mencurigakan dapat dimasukkan ke dalam daftar blokir (*blacklist*) sehingga tidak dapat mengakses jaringan.

Pemeliharaan sistem juga dilakukan dengan memonitor penggunaan sumber daya router, seperti CPU dan trafik jaringan, untuk memastikan bahwa sistem tetap berjalan dalam kondisi stabil.

 ISSN:2302-8149
e-ISSN:2540-9719

Hal ini penting untuk menghindari terjadinya overload yang dapat mengganggu kinerja jaringan.

Selain itu, dilakukan evaluasi terhadap efektivitas firewall berdasarkan hasil pengujian yang telah dilakukan pada tahap sebelumnya. Evaluasi ini bertujuan untuk mengetahui apakah aturan firewall yang diterapkan sudah mampu mengurangi dampak serangan DDoS secara signifikan.

Dengan adanya tahap manajemen, sistem keamanan jaringan tidak hanya berhenti pada tahap implementasi, tetapi juga dikelola secara berkelanjutan sehingga dapat beradaptasi terhadap perkembangan ancaman keamanan jaringan.

Kondisi ini mengindikasikan bahwa keberhasilan sistem keamanan tidak hanya ditentukan oleh implementasi awal, tetapi juga oleh pengelolaan dan pemeliharaan yang berkelanjutan untuk menghadapi perkembangan ancaman jaringan di masa mendatang.

5 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, implementasi firewall pada router MikroTik terbukti efektif dalam meningkatkan keamanan jaringan serta memitigasi serangan *Distributed Denial of Service* (DDoS) secara signifikan. Pengujian yang dilakukan pada tiga kondisi, yaitu kondisi normal, saat serangan, dan setelah penerapan firewall, menunjukkan adanya perbedaan performa jaringan yang jelas. Pada kondisi normal, jaringan berada dalam keadaan stabil dengan throughput sekitar ±0.1 Mbps, delay kurang dari 1 ms, packet loss sebesar 0%, serta penggunaan CPU pada kisaran 3%. Namun, ketika terjadi serangan DDoS tanpa mekanisme filtering, terjadi lonjakan throughput hingga ±40 Mbps yang disertai peningkatan delay menjadi 5–15 ms serta packet loss sebesar ±20–30%, yang mengindikasikan terjadinya penurunan kualitas layanan jaringan secara signifikan. Selain itu, penggunaan CPU meningkat drastis hingga mencapai 99–100%, yang menunjukkan bahwa sistem mengalami overload akibat banyaknya paket yang harus diproses secara bersamaan. Setelah penerapan firewall MikroTik, kondisi jaringan menunjukkan perbaikan yang signifikan, di mana throughput dapat ditekan menjadi sekitar ±2 Mbps, delay kembali stabil di bawah 1 ms, packet loss menjadi 0%, serta penggunaan CPU kembali normal pada kisaran ±3%. Hal ini menunjukkan bahwa mekanisme firewall, khususnya melalui teknik filtering, pembatasan koneksi (*connection limit*), serta pemblokiran paket tidak valid (*drop invalid*), mampu mengontrol trafik jaringan secara efektif sehingga tidak seluruh trafik serangan diteruskan ke jaringan internal. Dengan demikian, firewall tidak hanya berfungsi sebagai sistem keamanan, tetapi juga berperan dalam menjaga stabilitas performa jaringan dengan mengurangi beban kerja perangkat. Meskipun hasil penelitian ini menunjukkan efektivitas yang tinggi, terdapat beberapa keterbatasan, yaitu pengujian yang hanya dilakukan pada satu jenis serangan DDoS (SYN Flood) serta belum mengintegrasikan metode deteksi tambahan seperti *Intrusion Detection System* (IDS) atau pendekatan berbasis *machine learning*. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan sistem keamanan yang lebih komprehensif dengan menggabungkan firewall dan IDS, serta melakukan pengujian pada berbagai jenis serangan DDoS dalam skenario jaringan yang lebih kompleks agar hasil yang diperoleh semakin representatif terhadap kondisi jaringan nyata.

Referensi

[1] BPK RI, “Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan berbasis Elektronik,” 2018.

[2] B. S. dan S. Negara, “Strategi Keamanan Siber Nasional dan Peran BSSN,” Badan Siber dan Sandi Negara, 2021.

[3] L. Chen and others, “*Mitigating DDoS Attacks in Cloud Environments: A Review and Future Directions*,” *Futur. Gener. Comput. Syst.*, Vol. 140, pp. 45–60, 2023, DOI: 10.1016/j.future.2023.03.017.

[4] Y. Zhang and others, “*A Survey on DDoS Attack Detection in SDN-based Networks*,” *Comput. Networks*, Vol. 223, p. 109567, 2023.

[5] F. Prasetyo, A. Hamzah, W. Agel, and R. O. F. Kusuma, “Impelementasi Sistem Keamanan Jaringan Mikrotik menggunakan *Firewall Filtering* dan *Port Knocking*,” *J. Sistim Inf. dan Teknol.*, Vol. 5, No. 4, pp. 82–87, 2023, DOI: 10.60083/jsisfotek.v5i4.329.

[6] E. Eben, M. Mukramin, and H. Abduh, “Pengembangan Manajemen Keamanan Jaringan Nirkabel (Wifi) menggunakan *Routerboard Mikrotik* dan *Firewall* pada SMK Kristen Palopo,”

 ISSN:2302-8149
e-ISSN:2540-9719

J. Inform. dan Tek. Elektro Terap., Vol. 12, No. 3, 2024, DOI: 10.23960/jitet.v12i3.4716.

[7] A. C. Dachi and H. Noprisson, "Model Implementasi *Firewall MikroTik* dalam Pengelolaan Trafik dan Keamanan Jaringan," *JSAI J. SCI. Appl. Informatics*, Vol. 8, No. 3, pp. 788–793, 2025, DOI: 10.36085/jsai.v8i3.7878.

[8] W. W. Purba and R. Efendi, "Perancangan dan Analisis Sistem Keamanan Jaringan Komputer menggunakan SNORT," *Aiti*, Vol. 17, No. 2, pp. 143–158, 2021, DOI: 10.24246/aiti.v17i2.143-158.

[9] M. N. Rokhman and et al., "Implementasi *Firewall Filter Rule* dan *RAW* sebagai Metode Pengamanan Jaringan pada Perpustakaan XYZ," *J. Elektrosista*, Vol. 11, No. 1, pp. 58–75, 2023, DOI: 10.63824/jtep.v11i1.142.

[10] F. I. Wijaya, M. Innuddin, and K. A. Latif, "Analisa Penerapan *Fitur Firewall* pada Mikrotik untuk mengamankan dari Serangan *Denial of Service (DoS)*," *Panthera J. Ilm. Pendidik. Sains dan Terap.*, Vol. 5, No. 3, pp. 570–592, 2025, DOI: 10.36312/panthera.v5i3.546.

[11] D. Firmansyah and H. Hidayat, "Analisis Performa Jaringan setelah Implementasi *Firewall* pada *Router Mikrotik*," *J. Teknol. dan Sist. Komput.*, Vol. 11, No. 1, pp. 34–41, 2024.

[12] A. N. Hairun, "Penerapan *Firewall* di *Router OS Mikrotik* untuk mengantisipasi Serangan *DoS*," *J. Jar. dan Inform.*, 2023.

[13] R. Sulaiman, A. M. Raya, L. Laurentinus, and P. Padli, "Pemanfaatan *Mikrotik RB942-2ND* menggunakan Metode *Firewall Filtering* untuk Keamanan Jaringan dengan Model Forensikk," *J. Teknol.*, Vol. 17, No. 1, pp. 65–71, 2024, DOI: 10.34151/jurtek.v17i1.4725.

[14] T. Rahman and R. C. Wardoyo, "Pengembangan *Firewall Mikrotik* dalam *Blocking* Akses untuk meningkatkan Keamanan Jaringan Kantor Desa Cibalandong Subang," *J. Ilm. Sinus (JIS*, Vol. 23, No. 1, p. 15, 2025, DOI: 10.30646/sinus.v23i1.853.

[15] H. A. Al Kautsar and R. Sastra, "Implementasi *Firewall Mikrotik* dalam Pembatasan Akses Situs Terlarang di RT/RW Net," *Comput. SCI.*, Vol. 5, No. 2, pp. 123–132, Jul. 2025, DOI: 10.31294/coscience.v5i2.8897.

[16] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, "Implementasi *Firewall* pada *Mikrotik* untuk Keamanan Jaringan," *J. JOCOTIS-Journal SCI. Inform. Robot. E*, Vol. 1, No. 2, pp. 63–80, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[17] S. Kenat, "Analisis Keamanan Jaringan menggunakan Mikrotik pada Lab Komputer STMIK Widuri," *Neptunus J. Ilmu Komput. dan Teknol. Inf.*, Vol. 2, No. 3, pp. 16–24, 2024, DOI: 10.61132/neptunus.v2i3.177.

[18] A. K. Tahirou, K. Konate, and M. M. Soidridine, "*Detection and Mitigation of DDoS Attacks in SDN using Machine Learning (ML)*," *Proc. - 2023 Int. Conf. Digit. Age Technol. Adv. Sustain. Dev. ICDATA 2023*, Vol. 11, pp. 52–59, 2023, DOI: 10.1109/ICDATA58816.2023.00019.

[19] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "*Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study*," *J. Inf. Secur. Appl.*, Vol. 50, No. 3, 2020, DOI: 10.1016/j.jisa.2019.102419.

[20] S. K. Singh, "*Machine Learning-based DDoS Detection Techniques*," *IEEE Access*, Vol. 8, 2020, DOI: 10.1109/ACCESS.2020.2988452.

[21] H. T. Nguyen, T. V Phan, and N. H. Tran, "*A Deep Learning Approach for DDoS Attack Detection in Software-Defined Networking*," *Futur. Gener. Comput. Syst.*, Vol. 124, pp. 123–135, 2021, DOI: 10.1016/j.future.2021.05.003.

[22] M. Al-Fares and et al., "*A Survey of QoS in Network Performance Evaluation*," *IEEE Commun. Surv. Tutorials*, 2020, DOI: 10.1109/COMST.2020.2974748.

[23] S. Troia and et al., "*Performance Characterization and Profiling of Chained CPU-based Virtual Network Functions*," *Comput. Networks*, Vol. 225, 2023, DOI: 10.1016/j.comnet.2023.109628.

[24] R. Santosa, A. Haq, and M. Khanif, "*Comparative Analysis of Resource Utilization on 2.4 GHz and 5.8 GHz Wireless LAN Network Frequencies (OpenWrt Firmware Case Study)*," *J. Telecommun. Electron. Control Eng.*, Vol. 6, No. 2, pp. 176–187, 2024, DOI: 10.20895/jtece.v6i2.1394.