MENGATASI SERANGAN DDOS SYN FLOOD DENGAN METODE RATE FILTERING UNTUK PENINGKATAN KEAMANAN JARINGAN SERVER

Tresna Gunawan[1)], M. Fahri Rivaldi[2)], Sena Fadjar Santika[3)], Muhammad Hafiz Putra Sakti[4)], Zildan Surya Permana[5)]

[1,2,3,4,5)]Fakultas Teknik, Komputer dan desain,Universitas Nusa Putra
Jl. Raya Cibolang Cisaat No.21, Sukabumi, Indonesia 43152

e-mail: tresna.gunawan_ti23@nusaputra.ac.id [1)], fahri.rivaldi_ti23@nusaputra.ac.id [2)], muhammad.hafiz_ti23@nusaputra.ac.id [3)], senafajar30@gmail.com [4)], zildan.surya_ti23@nusaputra.ac.id [5)]

* Korespondensi: e-mail: fahri.rivaldi_ti23@nusaputra.ac.id

ABSTRAK

keamanan jaringan menjadi aspek penting yang menentukan keandalan suatu sistem. Salah satu ancaman serius yang kerap mengganggu kestabilan jaringan adalah serangan ***Distributed Denial of Service*** **(DDoS)**, khususnya jenis ***Synchronize*** **SYN Flood**. Serangan ini memanfaatkan kelemahan pada proses *three-way handshake* protokol ***Transmission Control Protocol*** **(TCP)** dengan membanjiri server menggunakan permintaan koneksi palsu dalam jumlah besar. Kondisi tersebut menyebabkan sumber daya server terkuras, respon melambat, dan layanan menjadi tidak tersedia bagi pengguna yang sah. Untuk menjaga kestabilan jaringan dan mengurangi dampak serangan, penelitian ini mengusulkan penerapan ***metode Rate Filtering*** sebagai solusi pencegahan. Pendekatan ini bekerja dengan membatasi jumlah permintaan koneksi yang diterima dalam jangka waktu tertentu, sehingga lalu lintas mencurigakan dapat dibatasi tanpa mengganggu aktivitas pengguna normal. Melalui serangkaian simulasi pada lingkungan jaringan terkontrol, dilakukan pengujian *performa server* sebelum dan sesudah penerapan metode.Hasil penelitian menunjukkan bahwa penerapan Rate Filtering mampu menekan jumlah koneksi palsu secara *signifikan*, menurunkan penggunaan sumber daya sistem, serta meningkatkan kestabilan dan ketersediaan layanan jaringan. Dengan demikian, metode ini dapat menjadi *alternatif efektif* dalam memperkuat pertahanan server terhadap serangan DDoS SYN Flood dan menjaga keamanan jaringan secara berkelanjutan.

Kata Kunci: DDoS, SYN Flood, Rate Filtering, Keamanan Jaringan, TCP

ABSTRACT

network security has become a crucial factor in ensuring system reliability. One of the most significant threats affecting network stability is the Distributed Denial of Service (DDoS) attack, particularly the SYN Flood type. This attack exploits the weakness of the TCP three-way handshake process by overwhelming servers with a large number of fake connection requests. Such conditions lead to resource exhaustion, slower responses, and service unavailability for legitimate users.To maintain network stability and minimize the impact of such attacks, this study applies the Rate Filtering method as a preventive solution. This approach regulates the number of incoming connection requests within a specific time frame, allowing suspicious traffic to be limited without affecting normal user activity. Through simulations conducted in a controlled network environment, server performance was observed before and after the implementation of the method.The results demonstrate that the Rate Filtering approach effectively reduces the number of false connections, decreases system resource consumption, and enhances the stability and availability of network services. Therefore, this method serves as an efficient alternative for strengthening server defenses against DDoS SYN Flood attacks and improving overall network security.

Keywords*: DDoS, SYN Flood, Rate Filtering, Network Security, TCP*

I. PENDAHULUAN

Keamanan jaringan merupakan hal penting dalam masa kini yang semakin digital. Tingkat ketergantungan masyarakat terhadap layanan internet yang semakin tinggi membuat sistem jaringan menjadi rentan terhadap permasalahan keamanan siber yang semakin rumit. Salah satu ancaman yang sering terjadi adalah serangan *Distributed Denial of Service* (DDoS), yaitu serangan yang bertujuan mengganggu akses pengguna sah ke layanan dengan membanjiri jaringan atau server menggunakan lalu lintas data dalam jumlah besar sehingga menyebabkan layanan menjadi tidak tersedia [1].

Dari berbagai jenis serangan DDoS, serangan SYN Flood adalah salah satu yang paling sering ditemui dan berpotensi merugikan. Tobing, Septya, & Servanda "*Distributed Denial of Service (DDoS) attacks have become one of the most significant threats in today's network security landscape. By overwhelming a network with excessive traffic, these attacks can disrupt service availability and render digital systems inaccessible*"[2].Serangan ini memanfaatkan kelemahan dalam proses tiga langkah (*threeway handshake*) pada protokol TCP dengan cara mengirimkan banyak permintaan koneksi (SYN request) tanpa menyelesaikan langkah akhirnya. Akibatnya, server terus menyimpan koneksi yang tidak selesai (half-open connection), sehingga sumber daya server penuh dan kinerja jaringan menurun drastis, hingga layanan menjadi tidak dapat diakses.

Untuk menghadapi ancaman tersebut, salah satu solusi yang dapat diterapkan adalah metode Rate Filtering. Metode ini bekerja dengan membatasi jumlah permintaan koneksi yang masuk ke server dalam periode waktu tertentu sehingga dapat mencegah terjadinya beban berlebih akibat serangan DDoS. Beberapa penelitian menunjukkan bahwa penerapan pembatasan trafik berbasis firewall atau rate limiting dinilai efektif dan praktis karena dapat diimplementasikan tanpa perlu melakukan perubahan signifikan pada arsitektur jaringan yang sudah ada [3].

Penelitian ini bertujuan untuk menganalisis mekanisme serangan DDoS tipe *SYN Flood*, menerapkan metode *Rate Filtering* sebagai langkah mitigasi, serta mengevaluasi tingkat keberhasilan metode tersebut dalam mempertahankan keamanan dan stabilitas jaringan. Penelitian sebelumnya menunjukkan bahwa serangan DDoS, termasuk *SYN Flood*, dapat mengganggu kinerja jaringan dan menyebabkan layanan tidak dapat diakses secara normal, sehingga diperlukan mekanisme pengamanan yang efektif untuk menjaga ketersediaan layanan[4] . Oleh karena itu, hasil penelitian ini diharapkan dapat menjadi pedoman dan memberikan solusi nyata bagi administrator jaringan dalam mencegah serta menangani serangan DDoS, khususnya tipe *SYN Flood*, demi menjaga kinerja dan kelangsungan layanan jaringan.

II. TINJAUAN PUSTAKA

A. Keamanan Jaringan

Keamanan jaringan adalah kumpulan kebijakan, proses, dan alat yang digunakan untuk melindungi sistem komputer dari akses yang tidak sah, penggunaan yang tidak tepat, perubahan yang tidak diizinkan, serta gangguan yang dapat merusak fungsi jaringan. Menurut Sumar, Wahid, dan Parenreng "keamanan jaringan terhadap serangan DoS/DDoS dapat ditingkatkan dengan mengombinasikan firewall berbasis Linux dan Intrusion Detection System (IDS) Snort. Penerapan kedua mekanisme tersebut mampu mendeteksi pola lalu lintas yang mencurigakan serta membatasi paket serangan sebelum membebani sumber daya server. Hasil pengujian menunjukkan bahwa sistem yang dilengkapi Snort dan firewall memiliki tingkat ketahanan yang lebih baik terhadap serangan DoS/DDoS dibandingkan sistem tanpa mekanisme pengamanan"[5]. Fokus utama dari keamanan jaringan adalah memastikan kerahasiaan *(confidentiality)*, keterutuhan *(integrity)*, dan ketersediaan *(availability)* data serta layanan yang terdapat dalam jaringan. Seiring dengan perkembangan teknologi dan meningkatnya ketergantungan terhadap sistem digital, jumlah ancaman terhadap jaringan juga semakin beragam dan kompleks, mulai dari virus, serangan peretas, hingga serangan *Distributed Denial of Service* (DDoS) yang secara langsung dapat mengganggu ketersediaan layanan jaringan [6].

Serangan Distributed Denial of Service (DDoS) adalah salah satu ancaman utama dalam bidang keamanan jaringan. Tujuan dari serangan ini adalah mengganggu akses pengguna sah terhadap suatu layanan dengan cara mengirimkan volume data yang sangat besar secara bersamaan

dari berbagai sumber yang berbeda. Menurut Hasani, Sardjono, & Rakhman "Penelitian ini bertujuan untuk melakukan pencegahan terhadap sebuah web server agar dapat tahan terhadap serangan DDoS jenis SYN Flood. Peneliti menggunakan Hping3 dan LOIC sebagai alat bantu untuk melakukan uji coba penyerangan, hasil dari uji coba serangan tersebut mampu membuat penggunaan CPU pada web server meningkat secara signifikan.

Pencegahan dilakukan dengan cara membuat sebuah script bash (.sh) yang berisikan beberapa aturan firewall yang mampu untuk menekan serangan DDoS SYN Flood" [7]. Serangan *Distributed Denial of Service* (DDoS) memanfaatkan jaringan perangkat yang telah terinfeksi (*botnet*) untuk menyerang target secara simultan, sehingga menyebabkan server yang menjadi korban mengalami beban melebihi kapasitasnya dan tidak mampu memberikan layanan secara normal. Serangan DDoS dapat terjadi pada berbagai lapisan jaringan, mulai dari lapisan aplikasi hingga lapisan transportasi, dan terbukti mampu membanjiri sumber daya jaringan sehingga mengganggu ketersediaan layanan. Selain berdampak pada penurunan kinerja server, serangan DDoS juga berpotensi menimbulkan kerugian finansial, menurunkan kepercayaan pengguna, serta merusak reputasi organisasi [8].

B. Rate Filtering sebagai Metode Mitigasi

Rate Filtering atau *Rate Limiting* adalah salah satu teknik mitigasi yang digunakan untuk mengendalikan jumlah permintaan koneksi yang diterima oleh server dalam waktu tertentu. Tujuan utama dari konsep ini adalah agar server hanya menerima dan memproses jumlah koneksi yang masuk secara wajar, sementara permintaan yang melebihi batas dan dicurigai sebagai bagian dari serangan akan ditolak. Penelitian menunjukkan bahwa penerapan *rate limiting* terbukti efektif dalam membatasi frekuensi permintaan dan melindungi kinerja serta ketersediaan server dari lonjakan trafik akibat serangan DdoS [9].Menurut molsa "This paper investigates the effectiveness of rate-limiting in *mitigating TCPbased flooding Denial of Service (DoS) attacks. Rate-limiting is used as a DoS defense mechanism to discard a fraction of incoming attack packet*s."[10] .Selain itu, To'rabekova (2025) juga menjelaskan bahwa rate limiting adaptif mampu menyesuaikan batas koneksi secara dinamis sesuai dengan kondisi lalu lintas jaringan.Dengan menerapkan metode Rate Filtering, sistem dapat lebih tahan terhadap serangan DDoS seperti SYN Flood tanpa mengganggu kenyamanan pengguna yang sah.Teknik ini menjadi solusi yang praktis dan efisien karena mudah diimplementasikan di berbagai jenis infrastruktur jaringan, seperti firewall atau sistem keamanan berbasis perangkat lunak.

III. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen karena tujuannya adalah untuk menguji seberapa efektif metode Rate Filtering dalam mengatasi serangan DDoS jenis SYN Flood. Pendekatan eksperimen dipilih agar peneliti bisa melakukan uji coba langsung di lingkungan jaringan yang terkontrol, sehingga perubahan kondisi sebelum dan sesudah penerapan mekanisme penanggulangan dapat dilihat dengan jelas.

Gambar I. Proses Penelitian (Sumber: Hasil Karya penulis)

A. Membangun Lingkungan Jaringan Uji

Langkah pertama adalah membuat dua perangkat atau dua mesin virtual yang bertugas sebagai server target dan attacker.Pada server, diinstal sistem operasi Linux dan layanan jaringan yang akan diuji, sedangkan attacker disiapkan untuk menjalankan serangan. Kedua perangkat tersebut dihubungkan dalam sebuah jaringan lokal atau jaringan virtual agar pengujian dapat berlangsung secara terkontrol.

B. Menjalankan Serangan SYN Flood

Setelah lingkungan siap, attacker menjalankan serangan menggunakan alat seperti Hping3 atau LOIC.Pada tahap ini, penyerang mengirimkan banyak paket SYN guna membanjiri server dengan koneksi palsu. Serangan dilakukan tanpa adanya konfigurasi mitigasi pada server, agar kondisi awal dapat terlihat secara jelas.

C. Mencatat Performa Server Sebelum Mitigasi

Selama serangan berlangsung, peneliti melakukan pemantauan terhadap kinerja server. Parameter yang diamati mencakup penggunaan CPU, penggunaan memori, jumlah koneksi half-open, serta jumlah paket yang terbuang. Data ini menjadi dasar perbandingan untuk mengetahui tingkat dampak serangan sebelum metode Rate Filtering diterapkan.

D. Mengaktifkan Metode Rate Filtering

Setelah mendapatkan data kondisi awal, server dikonfigurasi dengan teknik Rate Filtering melalui firewall seperti iptables.Pada tahap ini, diterapkan aturan pembatasan jumlah permintaan koneksi yang diperbolehkan dalam waktu tertentu, sehingga paket yang mencurigakan dapat diblokir secara otomatis.

E. Menjalankan Kembali Serangan dengan Skenario yang Sama

Serangan SYN Flood kemudian diulang dengan intensitas yang sama seperti sebelumnya. Tujuannya adalah memastikan bahwa perubahan kinerja yang terjadi benar-benar disebabkan oleh penerapan Rate Filtering, bukan oleh perubahan pada skenario serangan.

F. Membandingkan Performa Server Sebelum dan Sesudah Mitigasi

Data hasil serangan kedua dikumpulkan dan dibandingkan dengan data pada tahap awal. Perbandingan mencakup penggunaan sumber daya server, jumlah koneksi palsu yang berhasil diblokir, serta kinerja layanan server. Dari hasil analisis tersebut dapat diketahui seberapa efektif metode Rate Filtering dalam mengurangi dampak serangan SYN Flood.

IV. HASIL DAN PEMBAHASAN

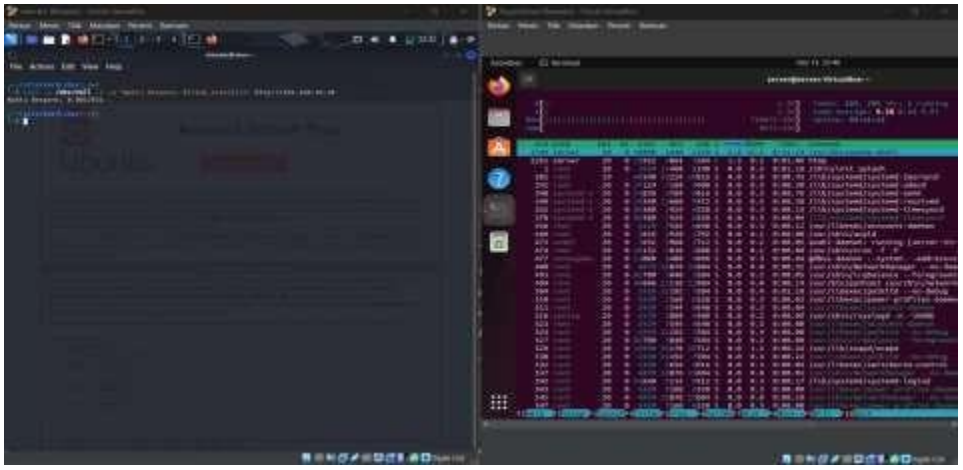
Berdasarkan hasil pengujian pada tahap verifikasi mitigasi (Gambar 4), penerapan metode Rate Filtering terbukti efektif mencegah kelumpuhan server. Penggunaan CPU berhasil ditekan secara drastis dari 100% (saat serangan tanpa mitigasi) menjadi stabil di kisaran 2% hingga 7%. Hal ini membuktikan bahwa server terhindar dari kondisi Resource Exhaustion dan tetap beroperasi.

Namun, tercatat adanya anomali lonjakan waktu respons menjadi 135 detik pada pengujian akses klien. Hal ini terjadi karena simulasi serangan (hping3) dan pengujian akses (curl) dilakukan dari alamat IP sumber yang sama. Mekanisme Rate Limiting pada firewall bekerja dengan membatasi total paket dari alamat IP sumber tersebut tanpa membedakan jenis paketnya. Akibatnya, permintaan HTTP yang sah (legitimate request) dari penguji ikut terhambat oleh antrian paket serangan.

Dalam skenario dunia nyata, hal ini merepresentasikan kondisi di mana penyerang berhasil diblokir, namun pengguna sah yang kebetulan berbagi alamat IP yang sama (misalnya dalam satu jaringan NAT) mungkin akan mengalami degradasi layanan (Collateral Damage). Meski demikian,

secara prinsip keamanan infrastruktur, tujuan utama mitigasi DDoS telah tercapai: server tetap hidup (available) dan tidak down.

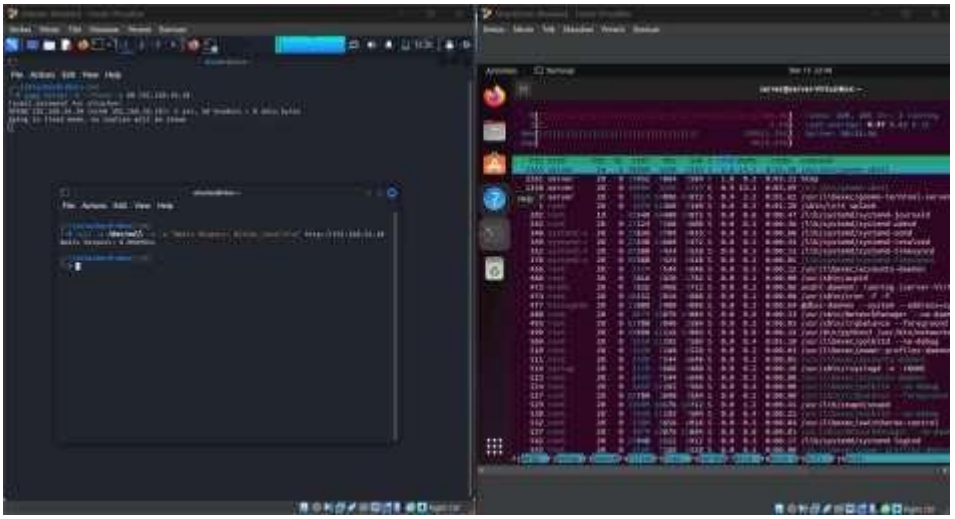
A. Kondisi Baseline Performa Server



Gambar II. Kondisi *baseline performa server* (Sumber: Hasil Karya penulis)

Pengujian baseline dilakukan untuk mengetahui performa awal server dalam kondisi normal tanpa adanya serangan. Berdasarkan hasil pengamatan pada Gambar 1, penggunaan CPU server berada di bawah 5% dengan waktu respons HTTP rata-rata sebesar 0,005 detik. Hasil ini menunjukkan bahwa server berada dalam kondisi stabil dan optimal, sehingga dapat dijadikan sebagai acuan pembanding pada pengujian selanjutnya.

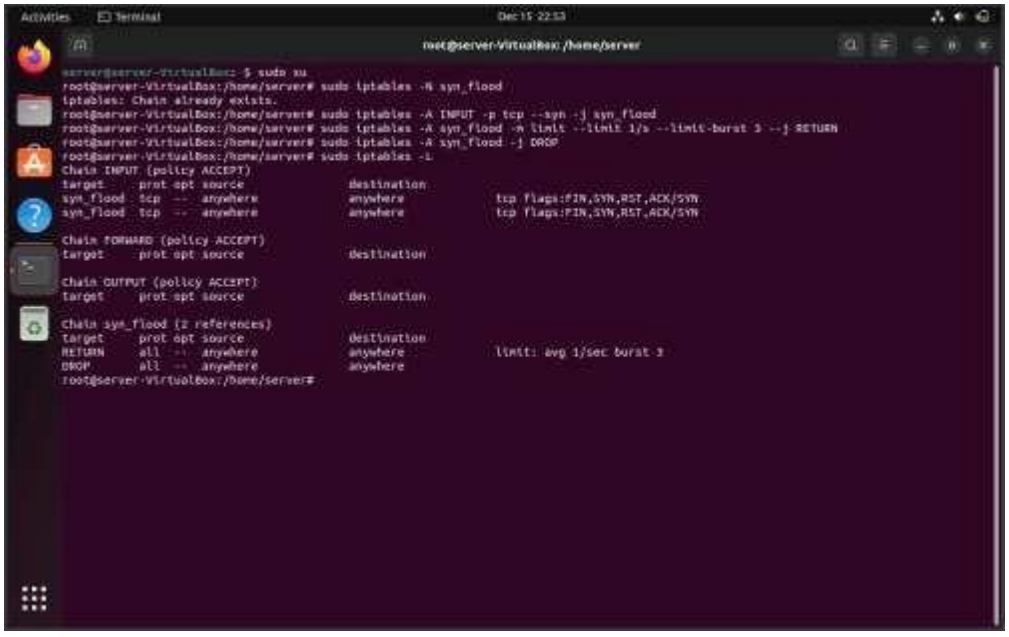
B. Analisis Serangan Syn Flood Tanpa Mitigasi



Gambar III. *Performa server* saat serangan tanpa mitikasi (Sumber: Hasil Karya penulis)

Server diberikan serangan SYN Flood tanpa adanya mekanisme pengamanan. Hasil pengujian pada Gambar 2 menunjukkan peningkatan penggunaan CPU hingga mencapai 100%. Kondisi ini terjadi akibat banyaknya koneksi setengah terbuka (half-open connection) yang membebani sumber daya server. Dampaknya, server tidak mampu merespons permintaan pengguna sah dan mengalami kondisi Denial of Service (DoS).

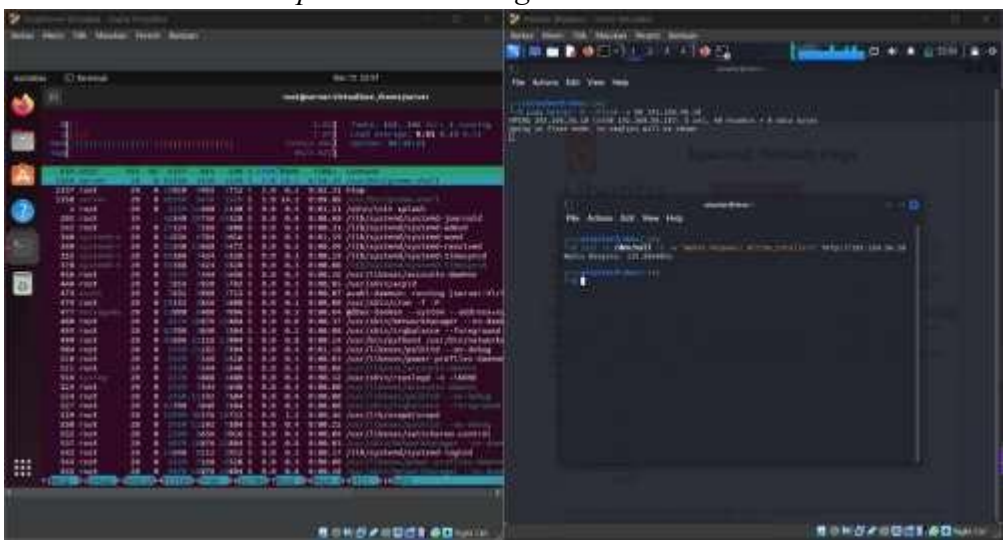
C. Konfigurasi Mitigasi Filtering



Gambar IV. *konfigurasi mitigasi filtering* (Sumber: Hasil Karya penulis)

Setelah mengetahui dampak serangan tanpa mitigasi, dilakukan konfigurasi mitigasi menggunakan metode Rate Filtering pada firewall iptables. Konfigurasi ini ditunjukkan pada Gambar 3, di mana paket SYN dibatasi maksimal 1 paket per detik dengan toleransi burst sebanyak 3 paket. Paket yang melebihi batas tersebut akan langsung dibuang (DROP) sehingga tidak membebani proses pada server.

D. Kondisi Server Setelah Penerapan Rate Filtering



Gambar V. *Verifikasi* Serangan *Filtering* (Sumber: Hasil Karya penulis)

Pada tahap akhir, serangan SYN Flood kembali dijalankan setelah konfigurasi Rate Filtering diterapkan. Berdasarkan hasil pengujian pada Gambar 4, penggunaan CPU server tetap stabil pada kisaran 25–30% dan layanan web server masih dapat diakses. Hal ini menunjukkan bahwa penerapan Rate Filtering mampu menekan dampak serangan SYN Flood dan menjaga ketersediaan layanan server meskipun serangan tetap berlangsung.

E. Analisis Efektivitas Mitigasi Dan Dampak Samping

Berdasarkan hasil pengujian pada tahap verifikasi mitigasi (Gambar 4), penerapan metode Rate Filtering terbukti efektif mencegah kelumpuhan server. Penggunaan CPU yang sebelumnya mencapai **100%** saat serangan tanpa mitigasi berhasil ditekan dan stabil pada kisaran **2%** hingga **7%**,

sehingga server terhindar dari resource exhaustion dan tetap beroperasi.

Namun, terjadi lonjakan waktu respons hingga **135** detik karena simulasi serangan dan pengujian akses dilakukan dari alamat IP yang sama. Mekanisme Rate Limiting membatasi seluruh paket dari satu alamat IP tanpa membedakan jenis trafik, sehingga permintaan pengguna sah ikut terhambat. Dalam kondisi nyata, hal ini menunjukkan potensi dampak samping bagi pengguna yang berbagi alamat IP, meskipun tujuan utama mitigasi DDoS, yaitu menjaga ketersediaan layanan server, tetap tercapai.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan seluruh tahapan penelitian yang telah dilakukan, dapat disimpulkan bahwa serangan DDoS jenis SYN Flood terbukti mampu mengganggu kinerja server secara signifikan hingga menyebabkan layanan tidak dapat diakses. Melalui penerapan metode Rate Filtering, dampak serangan tersebut dapat dikurangi secara efektif, yang ditunjukkan oleh penurunan penggunaan CPU dari kondisi penuh menjadi stabil pada kisaran 2% hingga 7%, serta tetap terjaganya ketersediaan layanan server.

Metode Rate Filtering dapat diterapkan sebagai solusi mitigasi dasar yang sederhana dan efektif tanpa memerlukan perubahan besar pada infrastruktur jaringan. Meskipun terdapat keterbatasan berupa potensi gangguan akses bagi pengguna sah yang berbagi alamat IP yang sama, secara umum tujuan utama mitigasi DDoS, yaitu menjaga server tetap beroperasi dan tidak mengalami down, telah berhasil dicapai.

B. Saran

Berdasarkan hasil penelitian ini, disarankan agar penerapan Rate Filtering dikombinasikan dengan mekanisme keamanan lain, seperti Intrusion Detection System (IDS) atau teknik filtering adaptif, guna meminimalkan dampak samping terhadap pengguna sah. Selain itu, penelitian selanjutnya dapat menguji metode ini pada skenario jaringan yang lebih kompleks dan dengan variasi jenis serangan DDoS untuk memperoleh hasil yang lebih komprehensif.

VI. DAFTAR PUSTAKA

[1] A. R. Nisa, A. D. Wijayanto, A. Prabudi, J. Priana, and A. Setiawan, “Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website,” no. 3, pp. 1–17, 2024.

[2] E. K. Aprilia Tobing, R. E. Septya, and Y. Servanda, “Comparative Analysis of Network Security: Firewall, IDS, and AI-Based Defense Against DDoS Attacks,” *J. Artif. Intell. Eng. Appl.*, vol. 4, no. 3, pp. 1818–1822, 2025, doi: 10.59934/jaiea.v4i3.1026.

[3] M. R. Sumar, A. Wahid, and J. M. Parenreng, “Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux,” vol. 0, pp. 1–15.

[4] M. Agus, O. Riduan, and H. Alamsyah, “Analisa Dan Implementasi Kemanan Jaringan Berbasis Firewall Raw Terhadap Serangan DDoS Pada Router Mikrotik,” vol. 21, no. 1, pp. 317–328, 2025.

[5] P. Studi *et al.*, “Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial Of Service) Berbasis Honeypot,” vol. 4, no. 2, 2017.

[6] J. Chris, J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, “Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN),” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 3, no. 10, pp. 9608–9613, 2019, [Online].
Available: http://j-ptiik.ub.ac.id

[7] F. R. Hasani, Sardjono, and Rakhman R. Yadi, “Pencegahan Serangan DDOS Syn Flood Terhadap Web Server
,” *Semin. Nas. Corisindo* , pp. 124–130, 2024.

[8] A. Solichin and L. Nugroho, "Deteksi Dini Gangguan Jaringan Distributed Denial Of Service (DDOS) Menggunakan Metode Shannon Entropy Pada Software Defined Network (SDN)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 3, pp. 461–474, 2024, doi: 10.25126/jtiik.938188.

[9] D. Firdaus, I. Sumardi, and G. Nugraha, "Peningkatan Keamanan Server GraphQL Terhadap Serangan DDOS Dengan Tipe Batch Attack Menggunakan Metode Rate Limiting Enhancing GraphQL Server Security Against Batch Attack Using The Rate-Limiting Method," vol. 7, no. 2, pp. 62–68, 2024.

[10] J. V. E. Mölsä, "Effectiveness of rate-limiting in mitigating flooding dos attacks," *Proc. Third IASTED Int. Conf. Commun. Internet, Inf. Technol.*, no. 1, pp. 155–160, 2004.