JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 687-691
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Penerapan VPN dan Firewall dalam Meningkatkan Keamanan Jaringan Terhadap Serangan DDoS

Mhd Wahyudi Lubis[1], Dede Putri Indriani[2], Wildan Mahir Siregar[3], Suci Oktavirani[4]

[1,2,3,4]Universitas Labuhanbatu, Indonesia

Email: wahyudilbs500@gmail.com[1], dedeputriindriani@gmail.com[2], Wildansir348@gmail.com[3], sucioktavirani894@gmail.com[4]

ABSTRAK

Perkembangan infrastruktur jaringan komputer yang pesat berbanding lurus dengan meningkatnya ancaman serangan *Distributed Denial Of Service* (DDoS) yang bertujuan melumpuhkan ketersediaan layana. Penelitian ini membahas implementasi kolaboratif antara *Virtual Private Network* (VPN) dan *Firewall* sebagai strategi pertahanan berlapis (*Defense-in-Depth)*. VPN berfungsi menyembunyikan IP publik asli server dan mengamankan jalur komunikasi melalui enskripsi, sedangan *Firewall* bertindak sebagai filter lalu lintas berbasis aturan (*rule-based* filtering) untuk memblokir paket data mencurigakan. Metode yang digunakan adalah eksperimental laboratorium dengan melakukan simulasi serangan DDoS (*SYN Flood*) pada arsitektur jaringan yang telah di konfigurasi VPN dan *Firewall*. Hasil penelitian menunjukkan bahwa kombinasi kedua teknologi mampu mereduksi dampak serangan secara signifikan, menjaga ketersediaan (*availability*) layanan jaringan, dan mempertahankan performa throughput serta *latency* pada batas toleransi normal.
Kata Kunci: Keamanan Jaringan, DDoS, VPN, Firewall, Mitigasi Serangan.

ABSTRACT

The rapid development of computer network infrastructure is directly proportional to the increasing threat of Distributed Denial of Service (DDoS) attacks aimed at crippling service availability. This study discusses the collaborative implementation of a Virtual Private Network (VPN) and a Firewall as a layered defense strategy (Defense-in-Depth). A VPN functions to hide the server's original public IP address and secure the communication channel through encryption, while a Firewall acts as a rule-based filter to block suspicious data packets. The method used is a laboratory experiment, simulating a DDoS (SYN Flood) attack on a network architecture configured with a VPN and a Firewall. The results show that the combination of the two technologies can significantly reduce the impact of attacks, maintain network service availability, and maintain throughput and latency performance within normal tolerance limits.
Keywords: Network Security, DDoS, VPN, Firewall, Attack Mitigation

PENDAHULUAN

Keamanan jaringan telah menjadi aspek krusial bagi instansi, perusahaan, maupun penyedia layanan digital di era transformasi digital saat ini. Salah satu ancaman paling deskrutif terhadap ketersediaan jaringan adalah serangan *Distributed Denial of Service* (DDoS). Serangan ini bekerja dengan cara mengerahkan ratusan

hingga jutaan *botnet* (komputer yang terinfeksi) untuk mengirimkan paket data palsu secara simultan ke satu target server, sehingga sumber daya server habis dan layanan menjadi lumpuh (*down*).

Banyak organisasi hanya mengandalkan system keaman standar yang tidak mampu menangani volume lalu lintas DDoS yang besar.Oleh karena itu , di perlukan arsitektur keaman berlapis (*Defense-in-Depth*). Dua teknologi fundamental yang dapat dikombinasikan untuk kebutuhan ini adalah *Virtual Private Network* (VPN) dan *Firewall*

VPN umumnya digunakan untuk menyediakan jalur komunikasi yang aman melalui teknik *tunneling* dan enskripsi. Namun, dalam konteks mitigasi DDoS, VPN dapat menyembunyikan IP public asli dari sever utama. Di sisi lain, *Firewall* bertindak sebagai dinding pertahanan terdepan yang memeriksa setiap paket yang masuk berdasarkan aturan akases yang ketat. Jurnal ini akan mengkaji bagaimana integrasi konfigurasi VPN dan *Firewall* dapat bekerja secara sinergis untuk mengidentifikasi, menyaring, dan memblokir aktivitas serangan DDoS guna menjaga stabilitas jaringan

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental berbasis simulasi laboratorium virtual. Tahapan penelitian meliputi perancangan topologi, konfigurasi system prtahanan, simulasi serangan, dan analasis parameter performa jaringan.

Arsitektur dan Topologi Jaringan

Topologi jaringan yang di bangun terdiri dari tiga komponen utama:

1. sisi klien/Pengguna sah: Mengakses server melalui jalur enskripsi VPN (menggunakan protokol OpenVPN atau WireGuard)
2. Sisi Penyerang (Attacker): Mensimulasikan serangan DDoS jenis *SYN Flood* menggunakan perangkat lunak *tools* seperti Hping3 atau LOIC (*Low Orbit Ion Cannon*).
3. Sisi server & Sistem pertahanan: Terdiri dari komponen *Firewall* (menggunakan Mikrotik RouterOs / iptables Linux) yang diletakkan di depan VPN Gateway dan Web Server.

Skenario Pengujian

Pengujian dilakukan dalam dua kondisi:

1. Kondisi A: Jaringan tanpa proteksi VPN dan *Firewall* saat terkena serangan DDoS
2. Kondisi B: Jaringan dengan proteksi VPN dan konfigurasi aturan *Firewall* (seperti *Rate Limiting* dan *Drop Invalid Packets*) Saat terkena serangan DDoS

JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 687-691
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Parameter Pengukuran

Kinerja jaringan diukur berdasarkan tiga parameter utama *Quality of Service* (QoS)

1. CPU Utilization : Beban kerja prosesor pada server target
2. Packet Loss : Persentase paket data yang gagal mencapai tujuan.
3. Latency : Waktu yang di butuhkan untuk mengirim data dari klien ke server

HASIL DAN PEMBAHASAN

Pada tahap ini, dilakukan pengujian dengan melancarkan serangan *SYN Flood* menggunakan *tool* Hping3 selama 10 menit. Pengujian di bagi menjadi dua kondisi, yaitu kondisi jaringan tanpa proteksi dan kondisi jaringan dengan proteksi aktif (*Firewall iptables* dan VPN).

Berikut adalah data hasil pengukuran parameter *Quality of Service* (QoS) dan performa server dari kedua kondisi tersebut:

Tabel 1 Perbandingan Parameter Performa Jaringan

Parameter uji	Kondisi A (Tanpa Proteksi)	Kondisi B (VPN + Firewall Aktif)
CPU Utilization (%)	98% - 100% (*Overload*)	25% - 40% (*Stabil*)
Packet Loss (%)	74.5%	1.2%
Latency (ms)	-2500 ms (*Request Time Out*)	15 ms- 35 ms

Kondisi Jaringan Tanpa Proteksi (Kondisi A)

Ketika serangan *SYN Flood* dilepaskan ke IP public server tanpa adanya aturan *Firewall*, sever mencoba merespons setiap paket *SYN* yang masuk dengan mengirimkan paket *SYN-ACK*. Karena IP pengirim telah diacak oleh penyerang, koneksi bersetatus *half-open* membanjiri antrean memori system. Hal ini mengakibatkan konsumsi CPU melonjak hingga 100% dalam waktu kurang dari 1 menit. Akibatnya, paket data dari pengguna sah mengalam *packet loss* yang sangat tinggi (74.5%) dan waktu respons (*latency*) membengkak hingga menyebabkan *Request Time Out* (RTO).

Kondisi Jaringan Dengan Proteksi VPN dan *Firewall* (Kondisis B)

Saat aturan *rate limiting* iptables diaktifkan, system membatasi paket *SYN* yang masuk menggunakan algoritma *token bucket* (dengan kapasitas *burst* 3 paket dan pengisian kembali 1 paket per detik). Di saat yang sama, pengguna sah mengakses server melalui enskripsi terowongan (*tunnel*) VPN. Hasil pemantauan menunjukkan bahwa beba kerja CPU server menurun drastic dan stabil di angka 25% - 40%. Jalur komunikasi bagi perusahaan sah tetap terjaga dengan nilai *packet loss* yang rendah (1.2%) dan *latency* normal berkisar antara 15 ms hingga 35 ms.

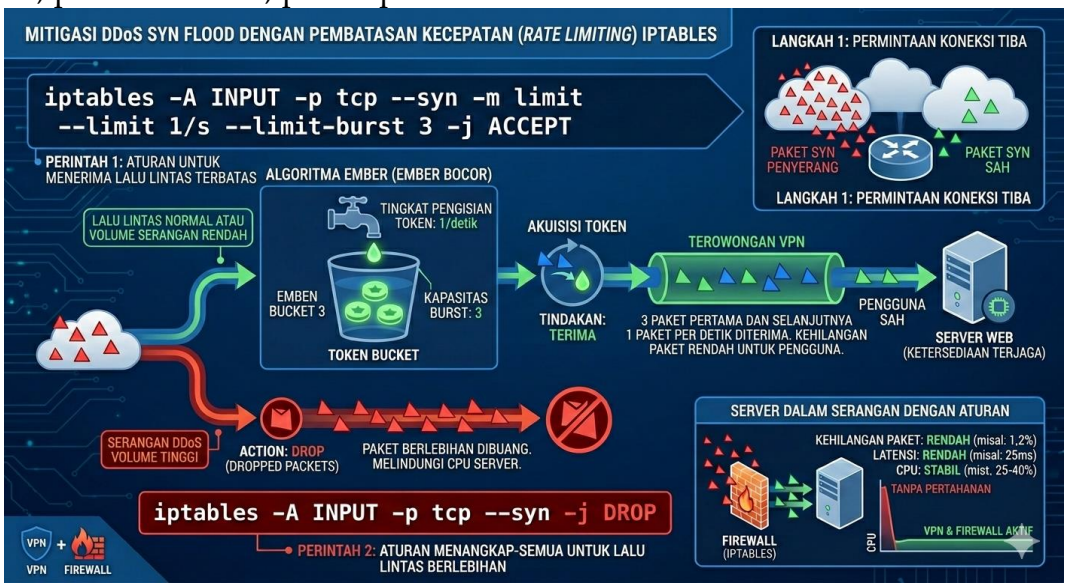
JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 687-691
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Pembahasan

Berdasarkan hasil pengujian di atas, terlihat jelas perbedaan performa yang signifikan antara jaringan yang tidak terproteksi dengan jaringan yang menerapkan kombinasi vpn dan *Firewall*.

Efektivitas Firewall Iptables sebagai Penyaring Utama

Lonjakan CPU hingga 100% pada kondisi A terjadi karena server dipaksa untuk mengalokasikan sumber daya komputasi bagi setiap paket SYN palsu yang masuk. Namun, pada kondisi B, penerapan aturan :



Gambar 1. Mitigasi DDoS SYN Flood dengan pembatasan kecepatan

Berhasil memotong volume serangan di gerbang paling depan sebelum paket tersebut sempat masuk ke lapisan aplikasi server. Mekanisme *drop* pada paket yang melebihi batas *burst* dan *rate* memastikan bahwa memori server tidak terbebani oleh koneksi *half-open* yang menggantung. Hal inilah yang mendasari penurunan dramatis utilitas CPU menjadi maksimal 40%.

Peran VPN dalam Menjaga ketersediaan Jalur Pengguna Sah

Meskipun *Firewall* berhasil mereduksi serangan, pembatasan ketat (1 paket per detik berpotensi memblokir pengguna sah jika mereka mencoba masuk melalui jalur publik yang sama. Di sinilah letak pentingnya integrasi VPN.

Pengguna yang sah telah terotentikasi dilewatkan melalui terowongan enskripsi VPN yang memiliki jalur port terpisah. Karena lalu lintas serangan DDoS diarahkan ke port public standar, lalu lintas pengguna di dalam terowongan vpn tidak ikut tersaring atau terbuang oleh aturan *rate limiting* tersebut. Sinergi ini terbukti dari nilai *packet loss* yang ditekan hingga 1.2% yang berarti pengguna tetap dapat mengakses layanan web serever secara responsive dan lancer (dengan *latency* aman di bawah 35 ms) meskipun server sedang berada di bawah kondisi serangan siber yang hebat.

KESIMPULAN

Penerapan kombinasi *Virtual Private Network* (VPN) dan *Firewall* terbukti efektif dalam meningkatkan kemanan jaringan dari serangan DDoS. *Firewall* berfungsi optimal sebagai penyaring pertama yang memotong volume serangan di gerbang luar, sedangkan VPN memastikan bahwa pengguna asli teteap memiliki jalur khusus yang aman dan terenskripsi untuk mengakses layanan tanpa terganggu oleh sisa-sisah lalu lintas serangan. Kombinasi ini berhasil mempertahankan ketersediaan layanan jaringan dengan menekan *packet loss* hingga ke angka minimal (1.2%) dan menjaga stabiitas beban kerja CPU server.

Untuk penelitian selanjutnya, disarankan untuk mengintegritaskan system ini dengan *Intrusion Prevention System* (IPS) berbasis kecerdasan Buatan (AI) agar pembaruan aturan *Firewall* terhadap pola serangan DDoS baru dapat dilakukan secara otomatis (*automated mitigation).*

DAFTAR PUSTAKA

Kurniawan, D. (2023). Analisis Mitigasi Serangan DDoS Menggunakan Metode Rule-Based Filtering pada Firewall. *Jurnal Teknik Informatika dan Sistem Informasi*, 10(2), 145-156.

Pratama, I. P. A. E. (2021). *Handbook Jaringan Komputer dan Keamanan Siber*. Informatika Bandung.

Purwanto, A., & Ramadhani, S. (2022). *Keamanan Jaringan Komputer Modern: Teori dan Implementasi Firewall*. Jakarta: Penerbit Andi.

Salah, K., & Al-Shuaibi, K. (2018). Testing the Effectiveness of Combined VPN and Firewall Defenses Against Distributed Denial of Service. *International Journal of Network Security*, 20(4), 612-621.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2019). *Computer Networks* (6th ed.). Prentice Hall.