Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 3354 – 3358 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

ANALISIS EFEKTIVITAS RAW FIREWALL MIKROTIK DALAM MITIGASI SERANGAN DDOS PADA INFRASTRUKTUR JARINGAN

Mhd Arfan Sitorus[1], **Darmeli Nasution**[2], **Muhammad Iqbal**[3]
Magister Teknologi Informasi, Universitas Pembangunan Panca Budi
e-mail: arfansyahgti@gmail.com

Abstract: *Distributed Denial of Service (DDoS) attacks pose a serious threat to the stability and availability of network services. MikroTik RouterOS provides a RAW Firewall feature as a DDoS attack mitigation method by filtering packets early on before they enter connection tracking. This study aims to analyze the effectiveness of using RAW Firewall on MikroTik in mitigating DDoS attacks on network infrastructure. The method used was a DDoS attack simulation using test equipment and configuring the RAW Firewall to block traffic indicated by the attack. Test results showed that implementing RAW Firewall reduced the router's CPU load by up to 35% during an attack compared to using a conventional firewall filter and maintained network bandwidth stability. This study is expected to serve as a practical reference for improving network resilience against DDoS attacks using MikroTik.*

Keywords: *DDoS, MikroTik, RAW Firewall, Mitigation, Network Security.*

Abstrak: Serangan Distributed Denial of Service (DDoS) merupakan salah satu ancaman serius terhadap stabilitas dan ketersediaan layanan jaringan. MikroTik RouterOS menyediakan fitur RAW Firewall sebagai salah satu metode mitigasi serangan DDoS dengan memfilter paket pada tahap awal sebelum masuk ke connection tracking. Penelitian ini bertujuan untuk menganalisis efektivitas penggunaan RAW Firewall pada MikroTik dalam mengatasi serangan DDoS pada infrastruktur jaringan. Metode yang digunakan adalah simulasi serangan DDoS menggunakan perangkat uji dan melakukan konfigurasi RAW Firewall untuk memblokir trafik yang terindikasi serangan. Hasil pengujian menunjukkan bahwa penerapan RAW Firewall mampu mengurangi beban CPU Router hingga 35% selama serangan berlangsung dibandingkan penggunaan filter firewall biasa, serta dapat mempertahankan stabilitas bandwidth pada jaringan. Penelitian ini diharapkan dapat menjadi referensi praktis dalam meningkatkan ketahanan jaringan terhadap serangan DDoS menggunakan MikroTik.

Kata kunci: DdoS, MikroTik, RAW Firewall, Mitigasi, Keamanan Jaringan.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong ketergantungan pada infrastruktur jaringan dalam berbagai sektor, termasuk pemerintahan, pendidikan, bisnis, dan layanan publik. Stabilitas dan ketersediaan jaringan menjadi aspek penting yang harus dijaga untuk memastikan kelancaran distribusi layanan digital kepada pengguna. Namun, seiring meningkatnya penggunaan jaringan, potensi ancaman serangan siber juga semakin tinggi, salah satunya adalah serangan Distributed Denial of Service (DDoS).

Serangan DDoS merupakan salah satu jenis serangan yang bertujuan untuk membuat layanan atau server menjadi tidak dapat diakses oleh pengguna dengan cara membanjiri target dengan lalu lintas data yang sangat besar dari berbagai sumber secara bersamaan. Hal ini dapat

menyebabkan penurunan performa layanan, downtime, hingga kerugian finansial bagi organisasi yang diserang. Oleh karena itu, diperlukan upaya mitigasi yang efektif untuk menghadapi serangan DDoS agar infrastruktur jaringan tetap stabil dan dapat melayani pengguna dengan baik.

MikroTik RouterOS sebagai salah satu perangkat jaringan yang banyak digunakan pada skala kecil hingga menengah menyediakan berbagai fitur firewall untuk pengamanan jaringan, salah satunya adalah fitur RAW Firewall. Fitur ini bekerja dengan melakukan filtering paket pada tahap awal sebelum masuk ke connection tracking, sehingga mampu mengurangi beban CPU router dan mencegah resource perangkat terkuras saat terjadi serangan DDoS. Dibandingkan dengan filter firewall konvensional, RAW Firewall memiliki keunggulan dalam efisiensi pemrosesan paket berbahaya secara cepat.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis efektivitas penggunaan RAW Firewall pada MikroTik dalam mitigasi serangan DDoS pada infrastruktur jaringan. Penelitian ini diharapkan dapat memberikan kontribusi sebagai referensi praktis bagi administrator jaringan dalam meningkatkan ketahanan jaringan menggunakan MikroTik RouterOS serta sebagai bahan evaluasi efektivitas penggunaan RAW Firewall dalam kondisi nyata saat serangan DDoS terjadi.

METODE

Penelitian ini dilaksanakan pada pridoe juni 2025 hingga juli 2025, tempat penelitian ini di lakukan di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Asahan, Dinas Kependudukan dan Pencatatan Sipil dipilih sebagai tempat penelitian dikarenakan Disdukcapil adalah dinas yang dimana banyak data pribadi masyarakat dikumpulkan dan di simpan, maka jika ada serangan *cyber* sangat mengancam keamanan data pribadi masyarakat di kabupaten asahan, penelitian ini bertujian untuk menganalisis seberapa efektif penggunakan raw firewall pada mikrotik untuk mengatasi serangan DDOS pada suatu jaringan.

Pada penelitian ini, serangan DDoS yang diterapkan adalah serangan DDoS ping flood. Serangan DDoS ping flood adalah serangan yang membanjiri ping ICMP atau request dari client ke router secara brutal, sehingga mengakibatkan cpu router menjadi overload dan down. Adapun konsep dari serangan DDoS Ping flood adalah user yang akan menyerangan terlebih dahulu sudah terhubung kejaringan router, hal ini bertujuan untuk mengetahui ip router yang sedang berjalan. Kemudian menyiapkan ping flood sebanyak mungkin untuk dilakukan ping massal yang ditujukan ke ip router, jika router tidak memiliki keamanan yang cukup, maka router akan menerima paket ping yang overload serta mengakibatkan router menjadi down hingga rusak (Wahyu Syahputra,T.M Diansyah,& Risko Liza 2020).

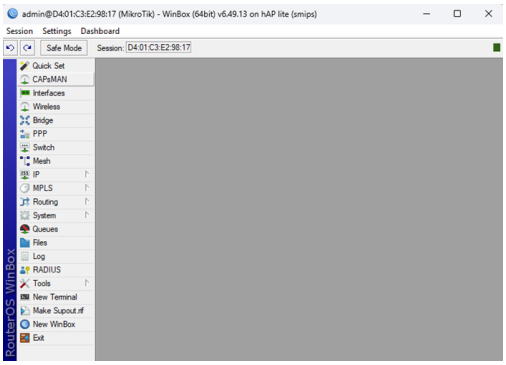
Penelitian ini menggunakan metode kuantitatif dengan menganalisis performasi dan kinerja dari Mikrotik apabila terjadi serangan(Bongga Arifwidodo , Yusup Syuhada , &Syariful Ikhwan2021), pendekatan kuantitatif dipipih karena penelitian ini berfokus pada analisis efektivitas penggunakan RAF Firewall dalam mengatasi serangan DDOS pada suatu struktur jaringan. RAW Firewall dapan mendeteksi trafik ICMP Flood yang terus menerus dalam waktu yang singkat, sehingga memungkinkan firewall dapan membelokkan trafik ICMP tersebut.

firewall adalah perangkat lunak atau perangkat keras yang digunakan untuk melindungi jaringan dengan menganalisis data yang masuk dan keluar, berdasarkan sekumpulan aturan, apakah memiliki rangkaian berbahaya atau tidak (Amien 2020). firewall adalah sebuah peranti keamanan yang berada di ujung koneksi internet

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 3354 – 3358 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

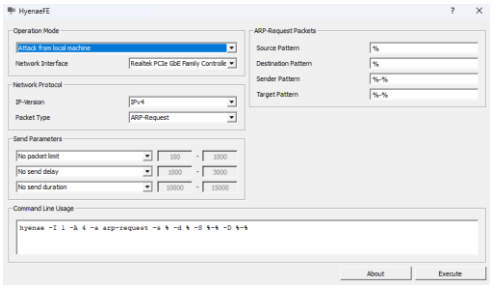
anda dan berfungsi sebagai Internet Broder Security Office (Petugas Keamanan Perbatasan Internet).Berdasarkan beberapa pengertian firewal menurut para ahli yang telah disebutkan di atas, dapat disimpulkan bahwa firewall merupakan perangkat lunak atau perangkat keras yang digunakan untuk melindungi jaringan dengan menganalisis data yang masuk dan keluar berdasarkan aturan tertentu (Noor dan Chandra 2020).

Pada penelitian ini menggunakan sofware dan hardware yang dimana itu mencakup winbox, dan hyenaeFE



Gambar 1. Winbox

Gambar diatas merupakan software yang di pergunakan agar pengguna bisa login pada mikrotik dan melakukan configurasi RAW Firewall dan melakukan mitigasi terhadap serangan DDOS,



Gambar 2. hyenaeFE

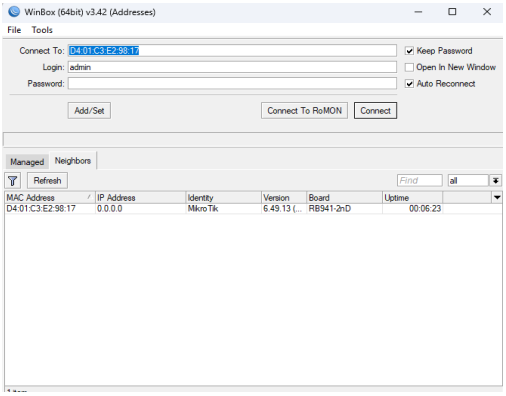
HyenaeFE adalah software boot yang akan mengirimkan trafik ICMP secara terus menerus, yang bisa menyebabkan overloard pada suatu perangkat, software ini akan kita jadikan simulasi serangan DDOS pada mikrotik,

HASIL DAN PEMBAHASAN

Pada tahap penting ini, penelitian melakukan konfigurasi RAW Firewall , dan melakukan analisi trafik sebelum melakukan configurasi RAW Firewall dan sesudah melakukan configurasi RAW Firewall.

1. Menu Login Winbox

Menu login digunakan untuk menampilkan koneksi mikrotik mana saja yang terhubung pada laptop, dan dapan melakukan login untuk masuk kedalam sistem operasi mikrotik



Gambar 3 *Menu Login Winbox*

2. Menu Data User

Menu data User untuk pengolahan data User di Dinas Komunikasi dan Informatika Kabupaten Asahan. Adapun menu data User adalah sebagai berikut.

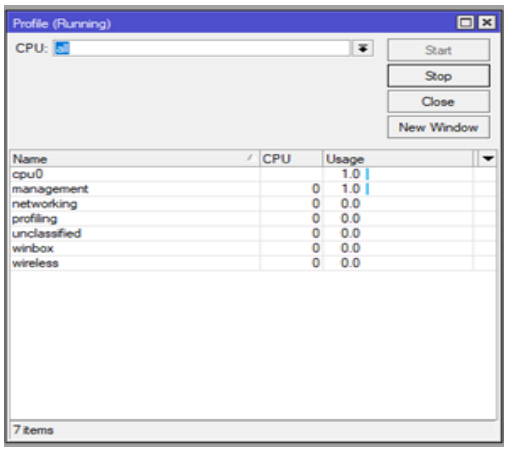
Gambar 4 *Tampilan Menu Winbox*

3. Menu Profile Winbox

Menu Profile berfungsi untuk monitoring semua performa pada mirkrotik, pada menu ini dapan memonitor kinerja yang cukup lengkap, dapat memonitor cpu, management, networking, profiling,

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 3354 – 3358 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

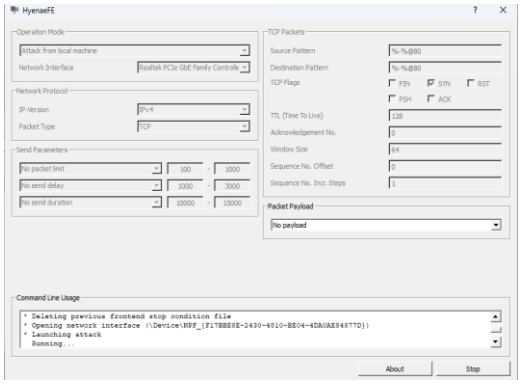
unclassified, winbox, dan wireless, pada bagian ini bisa terlihat bahwa usage cpu berada di 1.0 yang berarti kinerja cpu masih tergolong ringan.



Gambar 5 *Menu* Tools Profile

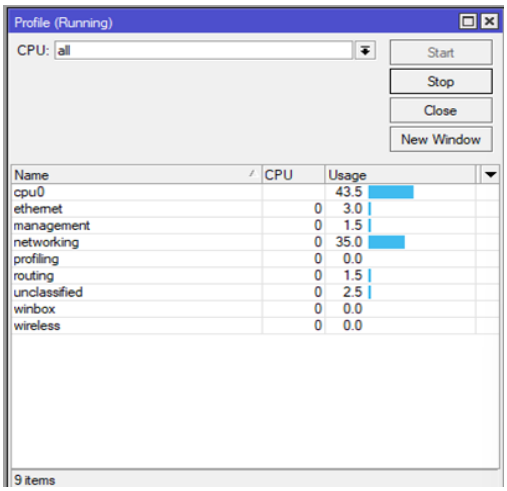
4. Hyenaefe Execute

Pada bagian ini penggunakan Hyenaefe untuk mengeksekusi tugasnya sebagai simulasi DDOS, yang di mana pada bagian ini memilih port apa yang kan kita serang, pada kali ini saya akan menyerang port Realtek PCIe Gbe, ip version IPv4, dan packet type TCP, dengan pengaturan seperti ini dapat di artikan, kita akan menyerang prot Realtek pcie, yang dimana port tersebut menggunakan IPv4, dan Packet yang akan kita kirim terus menerus mengguanakn Packet TCP.



Gambar 6. Hyenaefe setelah runing

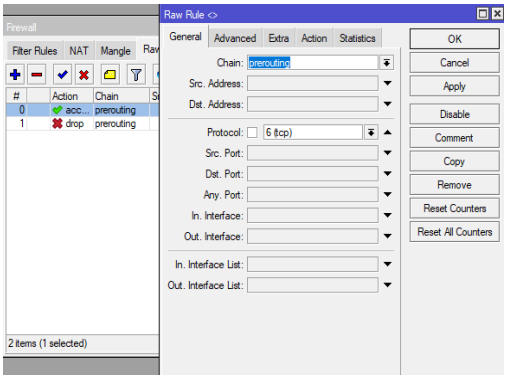
Pada gambar 7 dapat kita lihat tarafik yang meningkat sesaat hyenaefe melakukan simulasi DDOS, yang semulanya trafik cpu 1.0 dan netwoking 0.0, pada saat di lakuakn attack trafick cpu naik menjadi 43.5, dan netwoking naik menjadi 35.0



Gambar 7. Trafik setelah melakukan DDOS

5. Firewall

Untuk mengatasi DDOS kita akan meanfaatkan RAW Firewall, pada menu raw kita tambahkan dua RAW RULE, RULE yang pertama pada kolom chain kita menggunakan prerouting, dan pada protocol kita memilih 6tcp. Dan pada RULE kedua pada kolom chain kita menggunakan prerouting, dan pada protocol kita memilih 6tcp juga, tetapi pada menu action kita tambahkan action drop, yang dimana perintah drop itu akan memblokir trafik yang mencurigakan, yang dimana identifikasinya adalah trafik yang berulang dan dalam Waktu singgat melakukan pengiriman packet.



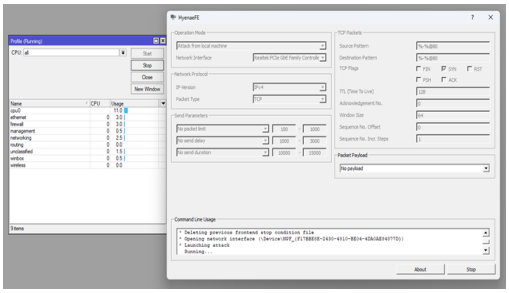
Gambar 8. Trafik setelah melakukan DDOS

6. Hasil

Pada gambar 9 kita bisa melihat pada saat Hyenaefe berjalan konfisi trafik usage cpu dan netwoking tergolong rendah, yaitu 11.0 dan 2.5, yang sebelumnya pada saat

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 3354 – 3358 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

Hyenaefe melakukan DDOS trafick cpu 43.5, dan netwoking 35.0



Gambar 9. Trafik setelah melakukan RAW Firewal

SIMPULAN

Berdasarkan hasil penelitian, penggunaan RAW Firewall pada MikroTik terbukti efektif dalam memitigasi serangan DDoS pada infrastruktur jaringan dengan memblokir paket berbahaya sebelum diproses lebih lanjut oleh filter firewall, sehingga mengurangi beban CPU dan bandwidth. Pengujian menunjukkan bahwa implementasi RAW Firewall dapat mengurangi trafik ilegal secara signifikan, menjaga stabilitas koneksi, serta mempertahankan ketersediaan layanan jaringan selama terjadi serangan. Dengan penempatan rule yang tepat pada RAW table, proses filtering berjalan lebih cepat dibandingkan filter firewall biasa karena paket dibuang sebelum diproses lebih jauh, sehingga meningkatkan efisiensi mitigasi. Namun, efektivitas mitigasi tetap dipengaruhi oleh konfigurasi rule yang tepat, pemantauan trafik secara berkala, serta penyesuaian dengan pola serangan terbaru untuk memastikan proteksi optimal terhadap infrastruktur jaringan.

DAFTAR PUSTAKA

Amien, Januar, A. 2020. Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knoking. Jurnal Fasilkom, Vol.10, NO.2, 159-165

Noor, Ermand, and Chandra, J.C. 2020. IMPLEMENTASI FIREWALL PADA SMP YADIKA 5 JAKARTA. Jurnal IDEALIS, Vol.3, No.1, 449-456

Asriyanto. (2021). Pemanfaatan Mikrotik Router Board sebagai pengaman serangan DDOS menggunakan metode IDS. *Garuda: Portal Garba Rujukan Digital*

Riduan, M. A., Riska, R., & Alamsyah, H. (2025, April 26). *Analisa dan implementasi keamanan jaringan berbasis Firewall RAW terhadap serangan DDoS pada Router Mikrotik*. Jurnal Media Infotama, 317–328.

A. H. Hendrawan, “Analisis serangan flooding data pada router MikroTik,” *Jurnal Krea-TIF*, vol. 4, no. 1, 2016.