Analisa Dan Implementasi Kemanan Jaringan Berbasis *Firewall Raw* Terhadap Serangan *DDoS* Pada *Router Mikrotik*

Mas Agus Okto Riduan[1], Riska[2], Hendri Alamsyah[3]

[1]Mahasiswa, Universitas Dehasen Bengkulu, Bengkulu, Indonesia
Alamat (Kampus I:Jl. Meranti Raya No.32 Sawah Lebar Kota Bengkulu; e-mail: masagusoktoriduan@gmail.com)
[2,]Dosen Tetap Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Kampus I: Jl. Meranti Raya No. 32 Sawah Lebar Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: riska.iskandar@unived.ac.id , hendrialamsyah@unived.ac.id)

(Received: Nopember 2024, Revised: Februari 2025, Accepied: April 2025)

Abstract*- This study aims to analyze and implement network security based on Raw Firewall against Distributed Denial of Service (DDoS) attacks on MikroTik Routers. DDoS is a serious threat that can disrupt network services, so it is important to test the effectiveness of Raw Firewall in dealing with these attacks. In this study, testing was carried out with three types of DDoS attacks, namely TCP SYN Flood, UDP Flood, and ICMP Flood, on local networks and internet networks. The research method used is an experimental method, where the Raw Firewall configuration is adjusted for various protocols being tested. The results showed that the raw firewall was able to block more than 70% of DDoS attack packets. In terms of performance before the raw firewall was activated, CPU usage on the router was 100% and free memory was 5.8 MiB when the attack occurred. When the Raw Firewall was activated, the CPU decreased to 60-70% and free memory increased to 9.8 MiB. In the DDoS test via the internet network also showed a decrease in CPU Load from 100% down to 5% and free memory from 4.5 MiB increased to 8.0 MiB. Quality of Service measurements showed no significant increase when the Raw Firewall was activated. This study concludes that the Raw Firewall is quite effective in blocking most packets from DDoS attacks. However, it has not been able to increase network stability because the network still experiences a decrease when the Raw Firewall is active.*
Keyword: DDoS, Mikrotik, Cyber, Network Security

I*ntisari- Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan keamanan jaringan berbasis Firewall Raw terhadap serangan Distributed Denial of Service (DDoS) pada Router Mikrotik. DDoS merupakan ancaman serius yang dapat mengganggu layanan jaringan, sehingga penting untuk menguji efektivitas Firewall Raw dalam menghadapi serangan tersebut. Dalam penelitian ini, pengujian dilakukan dengan tiga jenis serangan DDoS, yaitu TCP SYN Flood, UDP Flood, dan ICMP Flood, pada jaringan lokal dan jaringan internet. Metode penelitian yang digunakan adalah metode eksperimental, di mana konfigurasi Firewall Raw disesuaikan untuk berbagai protokol yang diuji. Hasil penelitian menunjukkan firewall raw mampu memblokir lebih dari 70% paket serangan DDoS. Dari sisi performansi sebelum firewall raw diaktifkan, penggunaan CPU pada router sebesar 100% dan free memory 5.8 MiB saat serangan terjadi. Ketika Firewall Raw diaktifkan, CPU menurun menjadi 60-70% dan free memory meningkat menjadi 9.8 MiB. Pada pengujian DDoS lewat jaringan internet juga menunjukkan penurunan CPU Load dari 100% turun menjadi 5% dan free memory dari 4.5 MiB meningkat menjadi 8.0 MiB. Pengukuran Quality of Service, menunjukkan tidak terlihat peningkatan yang signifikan saat Firewall Raw diaktifkan. Penelitian ini menyimpulkan bahwa Firewall Raw cukup efektif dalam memblokir sebagian besar paket dari serangan DDoS. Namun, belum mampu meningkatkan stabilitas jaringan karena jaringan masih mengalami penurunan saat Firewall Raw aktif.*
Kata kunci: DDoS, Mikrotik, Cyber, Keamanan Jaringan.

I. PENDAHULUAN

Dalam era di mana hampir setiap aspek kehidupan kita terhubung dengan internet, menjaga keamanan jaringan adalah hal yang sangat penting. Jumlah serangan siber yang terus meningkat menjadikan persoalan bagi penguna layanan internet. Berdasarkan laporan data dari badan siber dan sandi negara (BSSN) menunjukkan peningkatan jumlah serangan siber dari tahun ke tahun, tercatat ada 403 juta anomali trafik selama tahun 2023. Salah satu jenis anomali yang tercatat adalah serangan DDoS (Distributed Denial of Service). Serangan DDoS merupakan jenis serangan yang dilakukan attacker terhadap perangkat jaringan dengan cara menghabiskan resource yang dimiliki oleh perangkat jaringan atau server, sehingga tidak dapat menjalankan fungsinya dengan benar dan mencegah pengguna lain untuk memperoleh akses layanan sistem yang diserangnya. Serangan ini biasanya dilakukan dengan cara membanjiri jaringan target dengan lalu lintas data yang sangat besar, sehingga membuat perangkat jaringan atau server menjadi overload dan akhirnya tidak dapat berfungsi dengan baik. DDoS dapat menyebabkan gangguan serius bagi organisasi atau perusahaan, bahkan dapat menyebabkan kerugian finansial dan reputasi yang signifikan. Serangan DDoS dapat terjadi baik lewat jaringan internet maupun jaringan lokal, dan memiliki beberapa jenis metode penyerangan, seperti SYN Flood, ICMP Flood, dan UDP Flood Di tengah eskalasi serangan DDoS, perangkat jaringan seperti router, yang sering digunakan sebagai gateway utama untuk menghubungkan jaringan lokal dengan internet, menjadikan router sebagai target utama bagi para ettacker. Oleh karena itu, penting untuk memiliki sistem keamanan yang efektif untuk

P-ISSN 1858-2680
E-ISSN 2723-4673

melindungi router dari serangan DDoS. Untuk mengatasi masalah ini, dapat diterapkan dengan menggunakan sistem keamanan firewall. Firewall adalah sebuah perangkat keras atau perangkat lunak yang digunakan untuk mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Salah satu router yang banyak digunakan dan memiliki fitur ini adalah mikrotik routerboard. Pada mikrotik routerboard terdapat beberapa fitur firewall yang dapat digunakan untuk mengamankan jaringan, di antaranya adalah firewall filter rules dan firewall raw. Firewall filter rules dapat digunakan untuk memblokir aktivitas jaringan yang berpotensi membahayakan, seperti mencegah penggunaan aplikasi seperti Torrent, VPN, Port Scanning, hingga memblokir website. Sementara itu, firewall raw juga dapat melakukan blokir seperti halnya dengan firewall filter rules, namun dengan kosumsi resource yang lebih hemat. Hal ini dikarenakan Firewall raw memungkinkan melakukan bypass atau drop paket sebelum connection tracking, sehingga mengurangi resource dan meningkatkan efisiensi kinerja jaringan dibanding firewall filter rules. Pada penelitian sebelumnya, yang dilakukan (Fakhmi Mhd dan gultom 2021), serangan DDoS dengan tipe SYN Flood diujikan terhadap router mikrotik. Pada router mikrotik dilakukan konfigurasi pengamanan dari serangan DDoS menggunakan Firewall Raw, namun terdapat beberapa metode yang membutuhkan penyesuaian dan optimalisasi lebih lanjut. Beberapa aspek yang perlu diperhatikan adalah variasi jenis serangan DDoS yang belum sepenuhnya ditangani, dengan hanya fokus pada serangan SYN Flood dan mengabaikan jenis serangan lain seperti ICMP Flood dan UDP Flood. Karena keterbatasan ini, kesimpulan yang diambil dari penelitian ini, bahwa metode keamanan jaringan yang digunakan efektif dalam menangani serangan DDoS, menjadi kurang akurat. Oleh karena itu, diperlukan penelitian lanjutan yang mengadopsi beberapa penyesuaian dan peningkatan. Sehubungan dengan fungsi dan peran penting dalam jaringan, menyebabkan router memiliki potensi besar untuk menjadi target serangan DDoS. Oleh karena itu, dalam penelitian ini, tujuan utama penulis adalah untuk melakukan analisa terhadap pengamanan jaringan dari serangan DDoS yang dapat dilakukan menggunakan router mikrotik. Melalui penelitian ini, diharapkan dapat diperoleh pengamanan jaringan yang optimal dengan memanfaatkan fitur-fitur keamanan bawaan pada router mikrotik, serta mengetahui tingkat keefektifitasnnya berdasarkan pengaruhnya terhadap performa dari router tersebut. Berdasarkan latar belakang yang telah diuraikan, Maka penulis tertarik untuk mengambil judul "*Analisa dan Implementasi Keamanan Jaringan Berbasis Firewall Raw Terhadap Serangan DDoS Pada Router Mikrotik*".

II. TINJAUAN PUSTAKA

A. Analisa

Menurut Arifin et al (2021:2), analisa adalah sebuah cara dalam menyelesaikan suatu permasalahan dengan cara membaginya menjadi bagian-bagian yang saling berkaitan untuk memecahkan sebuah permasalahan demi terciptanya sebuah sistem yang akan diusulkan.

Menurut Fau et al (2017:12), analisa adalah merupakan suatu proses merinci terhadap objek dengan alat bantu tertentu, kedalam beberapa komponen yang saling berhubungan dengan menilai dan mengetahui perbedaan dari kedua objek tersebut yang berbeda.

Berdasarkan beberapa pengertian analisa menurut para ahli yang telah disebutkan di atas, dapat disimpulkan bahwa analisa merupakan suatu cara atau proses dalam menyelesaikan permasalahan dengan memecahnya menjadi bagian-bagian yang saling berkaitan.

B. Implementasi

Menurut Nasution (2024:47), implementasi adalah suatu prosedur atau serangkaian proses yang berkaitan dan diarahkan untuk mencapai suatu tujuan atau hasil tertentu. Menurut Anggraini et al (2023:186), implementasi adalah suatu rangkaian kerja sebuah alat yang digunakan dalam menyelesaikan sebuah masalah yang berkaitan dengan proses kerja, tujuannya adalah untuk menghasilkan hasil yang maksimal serta mengurangi kegagalan.

Menurut Burhanuddin dan Najeminur (2023:110), implementasi adalah teori pandangan bahwa interaksi bagian-bagian dengan bagian-bagian lainya dalam suatu eseluruhan atau sistem secara tanpa disengaja menghasilkan kegiatan atau fungsi-fungsi sesuai dengan tujuan.

P-ISSN 1858-2680
E-ISSN 2723-4673

Berdasarkan beberapa pengertian implementasi menurut para ahli yang telah disebutkan di atas, dapat disimpulkan bahwa implementasi merupakan suatu prosedur atau serangkaian proses yang diarahkan untuk mencapai tujuan atau hasil tertentu

D. Firewall

Menurut Amien (2020:160), 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.

Menurut Cahya et al (2023:65), firewall adalah teknologi keamanan siber yang digunakan untuk meningkatkan keamanan komputer yang terhubung ke jaringan, seperti jaringan Area Lokal (Lan) atau Internet.

Menurut Noor dan Chandra (2020:450), firewall adalah sebuah peranti keamanan yang berada di ujung koneksi internet 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.

E. DDoS

Menurut Harto Muhammad et al (2021:1330), DDoS adalah sekumpulan serangan Denial of Service yang memiliki lebih dari satu alamat traceback. Biasanya serangan DDoS menggunakan entitas botnet/zombies.

Menurut Mamuriyah et al (2024:163), DDoS adalah suatu jenis serangan yang dilakukan oleh suatu attacker yang bertujuan untuk membanjiri lalu lintas jaringan supaya menghabiskan sumber daya yang dimiliki oleh suatu komputer atau server.

Menurut Wahyuni dan adytia (2022:161), DDoS adalah sebuah metode serangan dengan mengirimkan banyak paket kedalam sebuah jaringan yang menyebabkan perangkat jaringan tidak berjalan sesuai fungsinya.

Berdasarkan beberapa pengertian DDoS menurut para ahli yang telah disebutkan di atas, dapat disimpulkan bahwa DDoS adalah serangan yang mengutamakan pembanjiran lalu lintas untuk merusak ketersediaan sumber daya komputer atau server, dengan metode pengiriman paket yang terus menerus dan melibatkan entitas seperti botnet atau zombies.

F. Mikrotik

Gambar 1 Mikrotik

Menurut Kurniawan et al (2023: 19), mikrotik adalah perangkat jaringan komputer yang berupa hardware dan software yang dapat difungsikan sebagai router, sebagai alat filtering, switching maupun yang lainya.

Menurut Ekawati dan Irwan (2021:42), mikrotik adalah perangkat jaringan komputer dengan beberapa fitur seperti bandwidth management, stateful firewall, hospot untuk akses plug and play, remote winbox GUI management, dan routing.

Menurut Sihotang et al (2020:230), mikrotik adalah sebuah merek dari sebuah perangkat jaringan, pada awalnya mikrotik hanyalah sebuah perangkat lunak atau software yang diinstall komputer yang digunakan untuk mengontrol jaringan..

Berdasarkan beberapa pengertian mikrotik menurut para ahli yang telah disebutkan di atas, dapat disimpulkan bahwa mikrotik adalah perangkat jaringan komputer yang berdiri dari hardware dan software.

III. METODOLOGI PENELITIAN

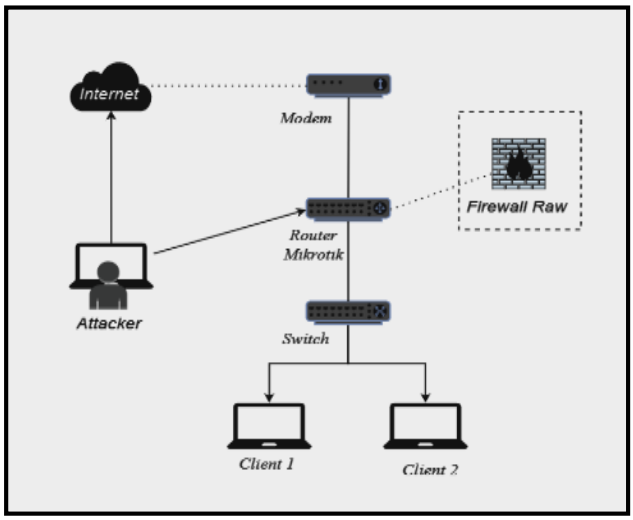
A. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode ekperimen. Metode ekperimen adalah pendekatan penelitian yang dirancang untuk menguji hipotesis atau mengeksplorasi hubungan sebab-akibat antara variabel-variabel tertentu. Dalam metode ini, penulis secara sengaja menerapkan suatu perlakuan atau intervensi tertentu pada kelompok subjek atau objek dalam lingkungan yang terkontrol, sambil mengontrol faktor-faktor lain yang mempengaruhi..

P-ISSN 1858-2680
E-ISSN 2723-4673

B. Diagram Blok Sistem Baru

Pada penelitan ini dilakukan pengembangan terhadap jaringan yang sudah ada dengan menerapkan keamanan jaringan berbasis Firewall raw terhadap serangan DDoS pada Router Mikrotik. Adapun topologi yang akan digunakan pada penelitian adalah sebagai berikut.



Gambar 2 Diagram Blok Sistem Baru

Pada gambar 2 terdapat 3 unit laptop, salah satunya adalah laptop attacker dan dua lainya laptop client, yang mana pada laptop attacker akan melakukan pengujian pada router Mikrotik dengan 2 metode penyerangan, yaitu melewati jaringan Internet dan jaringan lokal, menggunakan DDoS berjenis SYN Flood, UDP Flood dan ICMP Flood. Sementara itu, laptop client 1 akan mengonfigurasi Firewall Raw pada router Mikrotik dan melakukan pengujian kinerja pada router dengan menggunakan tools resource pada aplikasi Winbox. Pada laptop Client 2 akan melakukan pengukuran Quality Of Service sebelum dan sesudah konfigurasi Firewall Raw.

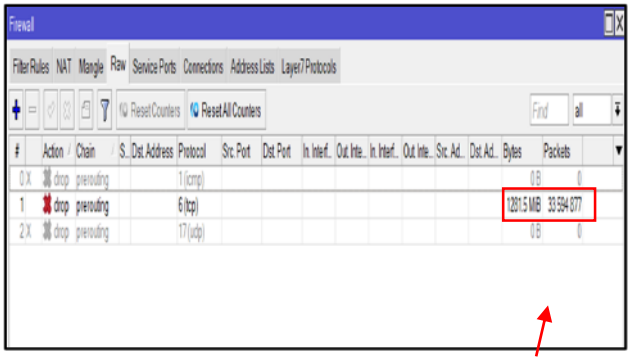
IV. HASIL DAN PEMBAHASAN

A. Hasil

Dari hasil penelitian yang dilakukan oleh penulis, mengenai bagaimana menganalisa dan implementasi keamanan jaringan berbasis Firewall Raw terhadap serangan DDoS pada Router Mikrotik, pada bab ini penulis akan menjelaskan hasil dari penelitian yang telah lakukan.

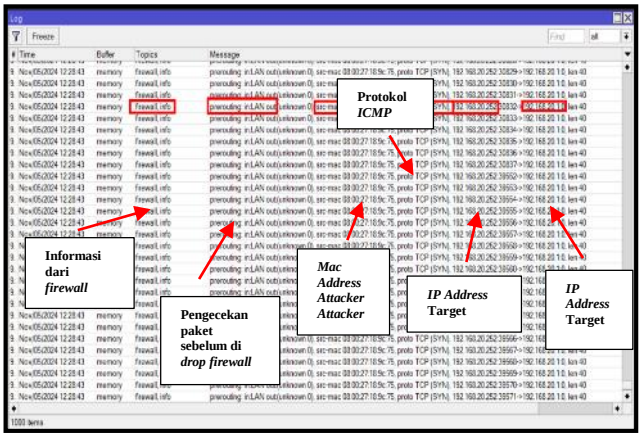
1. Hasil Serangan DDoS Pada Jaringan Lokal

a. Serangan TCP SYN Flood



Gambar 3 Paket Data Yang Berhasil Di

Pada Gambar di atas, terlihat bahwa sebanyak 33.594.877 paket dengan ukuran 1281.5 MiB dari total 48.075.479 (tidak semua paket berhasil masuk ke router mikrotik) yang dikirim oleh penyerang berhasil diblokir oleh firewall pada protokol TCP. Hasil ini menunjukkan bahwa sekitar 70% berhasil di atasi firewall raw Hasil pemblokiran dapat dilihat lebih jelas pada gambar berikut.



Gambar 4 Hasil Log

Pada gambar 4, log mencatat aktivitas pemblokiran paket oleh firewall di interface LAN (eth2). Terlihat bahwa paket-paket yang masuk dari IP sumber 192.168.20.252, yang merupakan IP perangkat attacker, diarahkan menuju IP target 192.168.20.1 menggunakan protokol TCP dan tipe paket SYN. Dalam log ini, Firewall Raw memproses paket-paket tersebut pada tahap prerouting untuk menentukan apakah paket tersebut akan diterima atau diblokir.

Tabel 1. Hasil Blokir Firewall RAW Jaringan Lokal

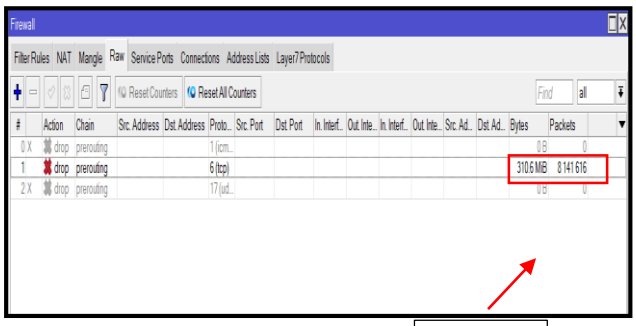
Jenis Serangan	Total Paket Dikirim	Total Paket yang di blokir Firewall Raw	Presentasi Blokir Firewall Raw
TCP Flood	48.075.479	33.594.877	69,9%
UDP Flood	46.545.455	30.192.786	64,9%
ICMP Flood	45.563.853	34.864.987	76,5%

P-ISSN 1858-2680
E-ISSN 2723-4673

2. Hasil Serangan DDoS Pada Jaringan Internet

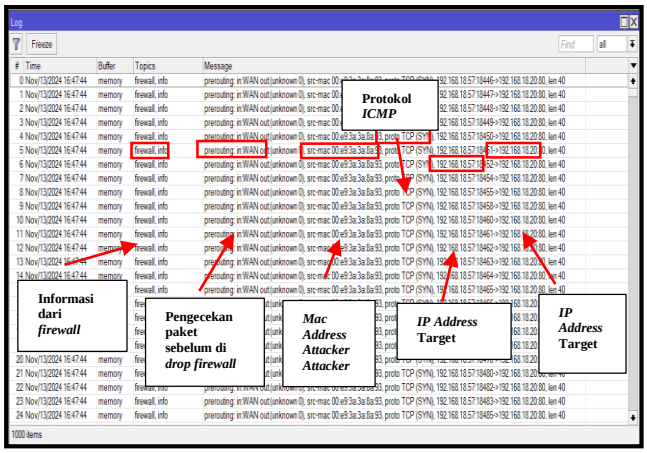
Pada pengujian ini, penulis menggunakan aplikasi hping3 di sistem operasi Kali Linux untuk melancarkan serangan DDoS pada jaringan internet dengan IP Address 192.168.18.20. Adapun hasil serangan DDoS pada Router Mikrotik dapat dilihat sebagai berikut

a. Serangan TCP SYN Flood



Gambar 5 Paket Data Yang Berha

Pada Gambar 5 di atas, terlihat bahwa sebanyak 8.141.616 dengan ukuran 310.6 MiB dari total 8.921.775 paket yang berhasil dikirim oleh attacker, diblokir oleh firewall pada protokol TCP lewat jaringan internet. Hasil ini menunjukkan bahwa sekitar 91% berhasil di atasi firewall raw. Hasil pemblokiran dapat dilihat lebih rinci pada gambar berikut.



Gambar 6 Hasil Log

Pada gambar 6 diatas, log mencatat aktivitas pemblokiran paket oleh firewall di interface WAN (eth1), terlihat bahwa paket-paket yang masuk dari IP sumber 192.168.18.57, yang merupakan IP perangkat attacker, diarahkan menuju IP target 192.168.18.20. melewati port 80 dengan menggunakan protokol TCP. Dalam log ini, Firewall Raw memproses paket-paket TCP tersebut pada tahap prerouting untuk menentukan apakah paket tersebut akan diterima atau diblokir.

Tabel 2. Hasil Blokir Firewall Raw Jaringan Internet

Jenis Serangan	Total Paket Dikirim	Total Paket yang di blokir Firewall Raw	Presentasi Blokir Firewall Raw
TCP Flood	8.921.775	8.141.616	91,24%
UDP Flood	3.905.161	3.688.006	94,44%
ICMP Flood	8.088.775	5.409.428	66,88%

3. Hasil Pengujian Penggunaan Sumber Daya Router Mikrotik

a. Hasil Pengujian Serangan DDoS Pada Jaringan Lokal

Pengujian sumber daya Router Mikrotik dilakukan untuk mengukur penggunaan sumber daya Router Mikrotik saat terjadi serangan DDoS jenis TCP SYN Flood, UDP Flood, dan ICMP Flood. Pengujian dilakukan menggunakan menu resource di aplikasi winbox selama 10 menit dengan interval pengambilan data setiap 1 menit untuk setiap jenis serangan, baik sebelum maupun setelah Firewall Raw diaktifkan. Adapun hasil pengujian dapat dilihat sebagai berikut

Tabel 3. Hasil Pengujian Serangan DDoS TCP Flood

Menit	CPU Load		Free Memory	
	Tanpa Firewall Raw	Dengan Firewall Raw	Tanpa Firewall Raw	Dengan Firewall Raw
1	100%	58%	5.3 MiB	9.7 MiB
2	100%	65%	5.5 MiB	9.7 MiB
3	99%	65%	4.9 MiB	9.7 MiB
4	100%	57%	4.8 MiB	9.5 MiB
5	100%	68%	4.7 MiB	9.5 MiB
6	100%	66%	5.5 MiB	9.7 MiB
7	100%	74%	5.6 MiB	9.7 MiB
8	100%	68%	5.6 MiB	9.7 MiB
9	100%	54%	5.6 MiB	9.6 MiB
10	100%	76%	5.6 MiB	9.9 MiB

Tabel 4. Hasil Pengujian Serangan DDoS UDP Flood

Menit	CPU Load		Free Memory	
	Tanpa Firewall Raw	Dengan Firewall Raw	Tanpa Firewall Raw	Dengan Firewall Raw
1	100%	69%	5.6 MiB	10.2 MiB
2	100%	64%	5.5 MiB	10.1 MiB
3	100%	60%	5.6 MiB	10.1 MiB
4	100%	57%	5.3 MiB	10.2 MiB
5	100%	55%	4.9 MiB	10.2 MiB
6	100%	71%	4.9 MiB	10.1 MiB

P-ISSN 1858-2680
E-ISSN 2723-4673

7	100%	69%	5.1 MiB	10.2 MiB
8	100%	67%	5.3MiB	10.2 MiB
9	100%	63%	5.3MiB	10.2 MiB
10	100%	63%	5.3 MiB	10.2 MiB

Tabel 5. Hasil Pengujian Serangan DDoS ICMP Flood

Menit	CPU Load		Free Memory	
	Tanpa Firewall Raw	Dengan Firewall Raw	Tanpa Firewall Raw	Dengan Firewall Raw
1	100%	69%	5.6 MiB	10.2 MiB
2	100%	64%	5.5 MiB	10.1 MiB
3	100%	60%	5.6 MiB	10.1 MiB
4	100%	57%	5.3 MiB	10.2 MiB
5	100%	55%	4.9 MiB	10.1 MiB
6	100%	71%	5.1 MiB	10.2 MiB
7	100%	69%	5.3 MiB	10.2 MiB
8	100%	67%	5.3 MiB	10.2 MiB
9	100%	63%	5.3 MiB	10.2 MiB
10	100%	63%	5.3 MiB	10.2 MiB

b. Hasil Pengujian Serangan DDoS Pada Jaringan Internet

Berdasarkan hasil pengujian yang sudah dilakukan penulis untuk menguji Firewall Raw dalam mengatasi serangan DDoS TCP SYN Flood pada jaringan internet, maka hasil penelitian tersebut akan disajikan menggunakan tabel sesuai dengan proses yang sudah dilakukan, dapat dilihat pada tabel 2 berikut.

Tabel 6. Hasil Pengujian Serangan DDoS TCP Flood

Menit	CPU Load		Free Memory	
	Tanpa Firewall Raw	Dengan Firewall Raw	Tanpa Firewall Raw	Dengan Firewall Raw
1	100%	9%	5.0 MiB	10.5 MiB
2	70%	11%	5.9 MiB	10.2 MiB
3	38%	5%	6.0 MiB	10.3 MiB
4	55%	9%	6.0 MiB	10.9 MiB
5	60%	7%	5.6 MiB	11.1 MiB
6.	74%	12%	5.6 MiB	11.3 MiB
7	36%	4%	5.8 MiB	11.9 MiB
8	70%	13%	5.9 MiB	11.1 MiB
9	80%	8%	5.6 MiB	11.3 Mib
10	40%	5%	5.6 MiB	11.5 MiB

4. Hasil Pengujian Kualitas Jaringan

a. Pengujian Kualitas Jaringan Pada Jaringan Lokal

Berdasarkan hasil pengujian yang sudah dilakukan, untuk menguji kualitas jaringan lokal pada saat serangan DDoS, sebelum dan sesudah Firewall Raw diaktifkan, maka hasil penelitian tersebut akan disajikan menggunakan tabel sesuai dengan proses yang sudah dilakukan, Adapun hasil dapat dilihat pada tabel 3 sebagai berikut.

Tabel 7. Hasil Pengujian Kualitas Jaringan

No	Jenis Serangan	Parameter QoS	Tanpa Firewall Raw	Dengan Firewall Raw	Keterangan
1	TCP Flood	Delay	25.57 ms	37.47 ms	Sangat Bagus
		Throughput	107 kb/s	49 kb/s	Sangat Bagus
		Jitter	1.68 ms	1.67 ms	Bagus
		Packet Loss	0%	0%	Sangat Bagus
2	UDP Flood	Delay	16.46 ms	16.46 ms	Sangat Bagus
		Throughput	166 kb/s	164 kb/s	Sangat Rendah
		Jitter	16.6 ms	1.63 ms	Bagus
		Packet Loss	0%	0%	Sangat Bagus
3	ICMP Flood	Delay	17.92 ms	15.86 ms	Sangat Bagus
		Throughput	144 kb/s	167 kb/s	Sangat Rendah
		Jitter	1.66 ms	1.66 ms	Bagus
		Packet Loss	0%	0%	Sangat Bagus

B. Pembahasan

Pada subbab ini akan dibahas mengenai alur kerja pada penelitian ini. Adapun rencana kerja dan persiapan alat serta bahan yang dibutuhkan pada penelitian ini adalah sebagai berikut.

1. Persiapan Alat dan Bahan

Adapun alat dan bahan yang disiapka, antara lain sebagai berikut:

1. 1 Mikrotik Routerboard RB941 -2ND
2. 3 Unit laptop
3. Modem
4. Switch
5. 5 Kabel UTP tipe Straight
6. Sistem Operasi Kali linux (diinstall melalui virtual box)
7. Hping3
8. Wireshark
9. WinBox

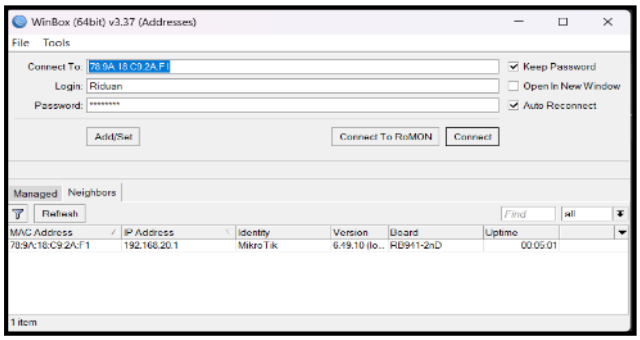
2. Konfigurasi Firewall Raw

Tahapan ini adalah tahapan awal sebelum melakukan pengujian terhadap keamanan jaringan menggunakan Firewall Raw pada Router Mikrotik. Adapun yang perlu dilakukan sebelum mengimplementasikan keamanan jaringan Firewall Raw dapat dilihat di gambar dibawah ini.

a. Buka Software Winbox di pc yang telah terhubung

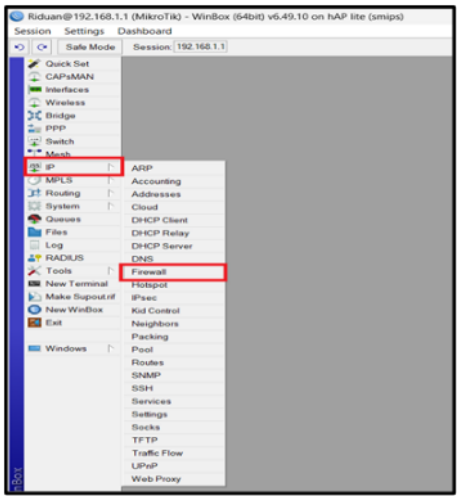
P-ISSN 1858-2680
E-ISSN 2723-4673

Router Mikrotik, lalu klik pada MAC Address atau IP Address lalu klik Connect. Seperti pada gambar di berikut



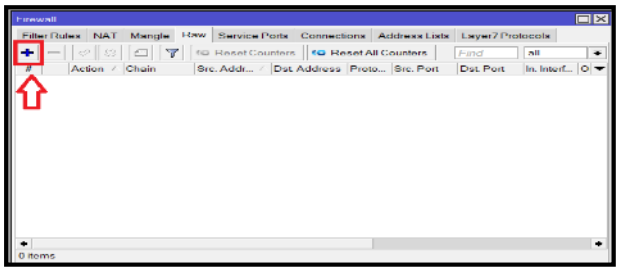
Gambar 7 Tampilan Login Winbox

b. Selanjutnya pada menu sebelah kiri pilih IP lalu cari kebawah dan pilih Firewall.



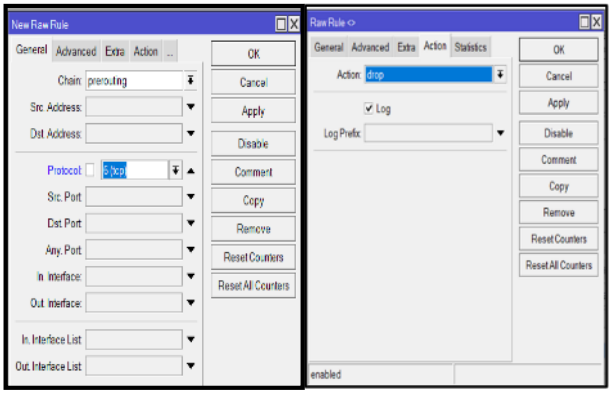
Gambar 8 Tampilan MenuWinbox

c.Selanjutnya pergi ke menu Raw lalu pilih tanda tambah (add).



Gambar 9 Tampilan Firewall Raw

d. Selanjutnya pada konfigurasi Firewall Raw, penulis menerapkan 3 konfigurasi yaitu dengan protokol TCP, UDP, dan ICMP. Lalu pada chain “prerouting” untuk memblokir semua paket TCP yang mencurigakan. Action drop diterapkan agar setiap paket yang memenuhi kriteria ini langsung dibuang sebelum mencapai jaringan internal, dan opsi log diaktifkan untuk mencatat setiap paket yang diblokir. Adapun hasil konfigurasinya dapat dilihat pada gambar di bawah.



Gambar 10 Konfigurasi Firewall Raw TCP

C. Hasil Pengujian Sistem

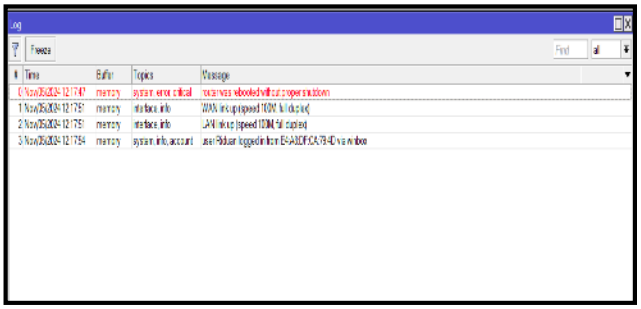
1. Pengujian Serangan DDoS pada Jaringan Lokal

a. Serangan *DDoS TCP Flood*

Proses pertama yang dilakukan adalah melakukan serangan DDoS sebelum Firewall Raw diaktifkan dengan menjalankan hping3 dengan perintah sudo hping3 -S --flood 192.168.20.1. Perintah tersebut digunakan untuk melakukan serangan SYN Flood ke perangkat Router Mikrotik dengan IP Address 192.168.20.1. Proses penyerangan DDoS SYN Flood dapat dilihat pada gambar berikut.

Gambar 11 Proses Serangan DDoS TCP Flood

Setelah melakukan serangan, selajutnya adalah melihat data trafik dan aktivitas pada log saat terjadi serangan tanpa Firewall Raw. Adapun hasil dapat hasilnya dapat dilihat pada gambar berikut

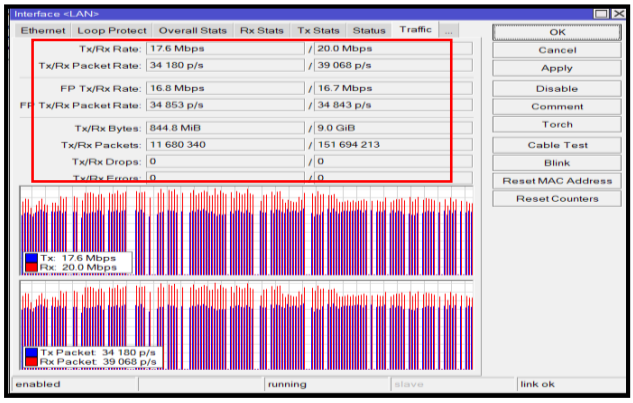


Gambar 12 Tampilan Log Sebelum Firewall Aktif

Pada gambar di atas, log menunjukkan bahwa tidak terdapat aktivitas mencurigakan atau berbahaya yang terdeteksi pada sistem sebelum Firewall Raw diaktifkan.

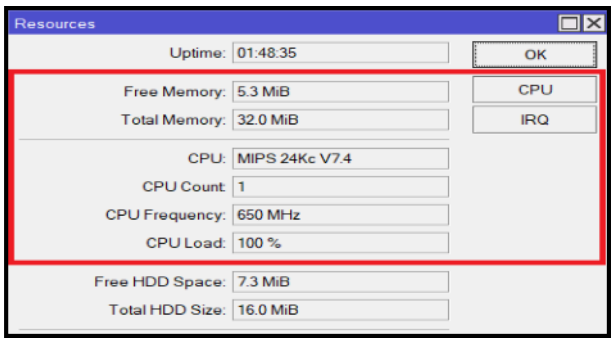
P-ISSN 1858-2680
E-ISSN 2723-4673

Kemudian keadaan traffic pada interface LAN, terlihat bahwa traffic terlihat tidak normal yang dimana nilai Tx/Rx Rate yaitu 17.6 Mbps / 20.0 Mbps dan nilai Tx/Rx Packet yaitu 34 180 p/s/39 068p/s. Hal ini menunjukkan bahwa Router menerima trafik masuk yang jauh lebih tinggi daripada yang dapat dikirim keluar. Total data yang diterima oleh interface mencapai 9.0 GiB, jauh lebih besar dibandingkan data yang dikirim 844.8 MiB, Adapun hasil traffic dapat dilihat pada gambar berikut.



Gambar 13 Traffic Interface Saat Serangan TCP Flood

Saat terjadi serangan DDoS, CPU Load dan Free Memory mengalami peningkatan. CPU Load meningkat secara signifikan menjadi 100% dan Free Memory berkurang menjadi 5.3 MiB. Hal ini yang dapat menyebabkan down pada jaringan Router. Adapun hasil resources dapat dilihat pada gambar berikut.

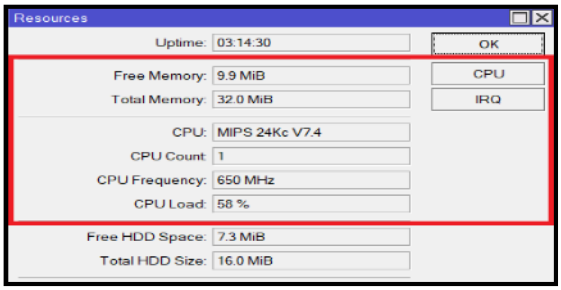


Gambar 14 Resources Setelah Terjadi Serangan DDoS

Dari hasil permasalahan diatas, penulis melakukan tindakan dengan memberhentikan serangan dan meningkatkan keamanan terhadap Router dengan mengaktifkan fitur Firewall Raw pada Router Mikrotik. Kemudian saat selesai mengaktifkan Firewall Raw, penulis melakukan serangan kedua kalinya. Adapun hasil serangan kedua dapat dilihat pada gambar berikut.

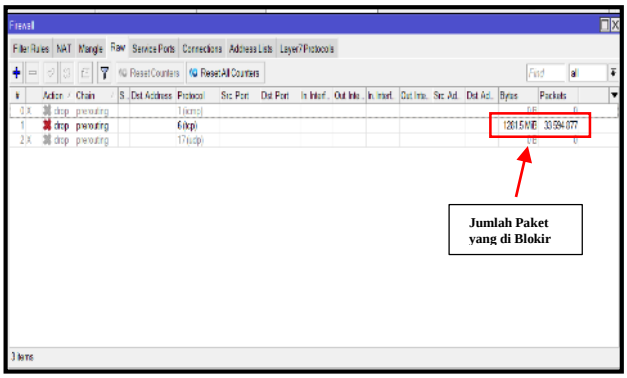
Gambar 15 Hasil Serangan DDoS TCP Flood

Setelah Firewall Raw aktif, penggunaan CPU turun menjadi 58% dan Free Memory meningkat menjadi 9.9 MiB. Hasil ini sangat berbeda dibandingkan dengan hasil sebelum nya ketika Firewall Raw belum diaktifkan. Adapun hasil dapat dilihat pada gambar berikut.



Gambar 16 Resources Setelah Firewall Raw Aktif

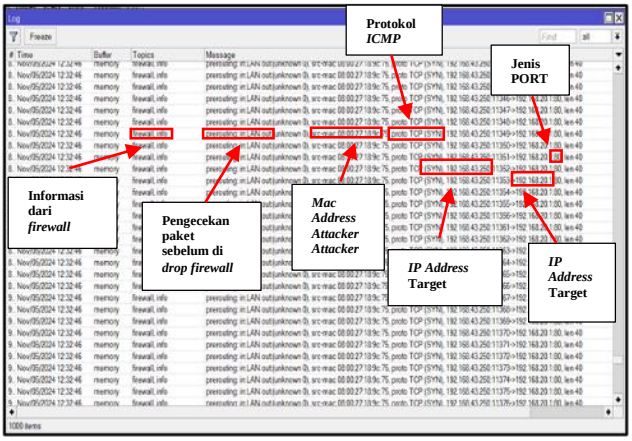
Pada Raw Rule menunjukkan bahwa paket yang dikirim sebanyak 48.075..479 oleh attacker, sebanyak 33.594.877 paket dengan ukuran 1281.5 MiB yang berhasil di drop oleh Firewall Raw. Hasil dapat dilihat pada gambar di bawah ini



Gambar 17 Raw Rule Firewall Raw

Untuk hasil dari data log, terlihat bahwa Firewall Raw berhasil mendeteksi dan memblokir serangan DDoS TCP SYN Flood yangmasuk lewat interface LAN menuju ke jaringan internet. Adapun hasil log dapat dilihat pada gambar berikut.

P-ISSN 1858-2680
E-ISSN 2723-4673



Gambar 18 Hasil Log Saat Firewall Raw Aktif

2. Pengujian Kualitas Jaringan

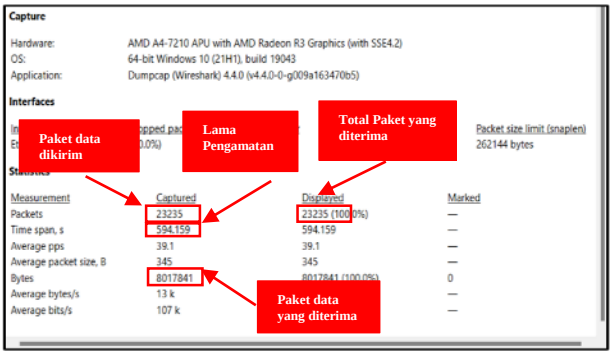
Pengujian kualitas jaringan dilakukan untuk menganalisis dampak serangan DDoS terhadap performa jaringan lokal dan jaringan internet, baik sebelum maupun setelah Firewall Raw di aktifkan. Serangan DDoS yang diuji meliputi TCP Flood, UDP Flood, dan ICMP Flood masing-masing selama 10 menit.

a . Pengujian Kualitas Jaringan pada jaringan lokal

Dalam pengujian ini parameter yang digunakan parameter Qos (Quality Of Service) seperti Throughput, Packet loss, Jitter, dan Delay didasarkan pada rekomendasi ITU-T G.1010 untuk mengukur kualitas layanan jaringan. Pengujian dilakukan menggunakan aplikasi wireshark dengan menerapkan Filter "ip.address = 192.168.20.1", Filter tersebut dikhususkan untuk memantau data yang keluar masuk yang melewati gateway.

1. Serangan DDoS TCP Flood

a. Sebelum Firewall Raw Aktif



Gambar 19 Hasil Capture Wireshark

Berdasarkan hasil capture data menggunakan aplikasi wireshark, seperti yang ditunjukkan pada Gambar 4.10 diatas, penulis dapat menganalisis dan menghitung nilai dari berbagai parameter quality of service (Qos). Berikut adalah perhitungan untuk masing-masing parameter QoS.

1. Throughtput

Throughtput merupakan jumlah total paket yang berhasil diterima di sisi klien/tujuan dalam periode waktu tertentu, dibagi oleh durasi periode tersebut. Dari data capture yang telah diperoleh menggunakan wireshark, throughtput dihitung dengan metode perhitungan berikut.

Throughtput = Paket data yang diterima / Lama Pengamatan

= 8017841/594.159 s

= 13494 Byte/s

= 13.494 Kb/s

= 107 Kb/s

2. Packet loss

Packet loss merupakan kondisi di mana satu atau lebih paket data yang dikirim melalui jaringan komputer gagal mencapai tujuan akhirnya. Dari data capture yang telah dilakukan dengan aplikasi wireshark maka nilai yang di dapatkan Packet loss dengan cara perhitungan sebagai berikut:

Packet loss = (Paket data dikirim – paket data diterima) x 100%

= (23235/23235) x 100

= 0%

3. Jitter

Jitter merupakan variasi dalam waktu kedatangan paket data saat ditransmisikan melalui jaringan. Ini adalah salah satu parameter kualitas layanan yang penting dalam jaringan komputer. Dari data Capture yang telah dilakukan dengan aplikasi wireshark maka didapatkan nilai Jitter dengan cara perhitungan sebagai berikut:

Jitter = Total variasi Delay / (Total Packet yang diterima -1)

= 39.1 / (23235-1)

= 0,00168 s

= 1.68 ms

4.Delay

Delay merupakan waktu yang dilakukan untuk sebuah paket data untuk melakukan perjalanan dari sumber ke tujuan melalui. Dari Capture yang telah dilakukan di

P-ISSN 1858-2680
E-ISSN 2723-4673

aplikasi wireshark maka di dapatkan nilai Delay dengan cara perhitungan sebagai berikut:

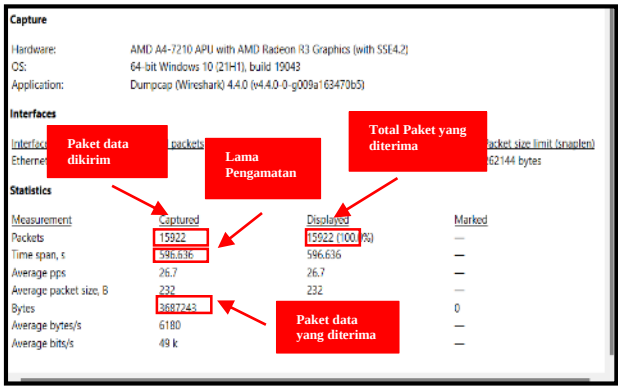
Rata-rata Delay = Total Delay / Total Packet yang diterima

= 594.159/23235

= 0.02557 s

= 25.57 ms

b. Serangan Sesudah Firewall Raw Aktif



Gambar 20 Hasil Capture Wireshark

a.Throughput

Throughput = Paket data yang diterima/Lama pengamatan

= 3687243/596.636 s

= 6180 Bytes/s

= 6.180 Kb/s

= 49 Kb/s

b. Packet loss

Packet loss = (Paket data yang dikirim – paket data yang diterima) x 100%

= 15922/15922

= 0 %

c. Jitter

Jitter = Total variasi Delay / Total paket yang diterima -1

= 26.7 / 15922-1

= 0.001677 s

= 1.67 ms

d. Delay

Delay = Total Delay / Total paket diterima

= 596.636 / 15922

= 37.472 s

= 37.47 ms

V.PENUTUP

A. Kesimpulan

Dari hasil penelitian yang dilakukan, dapat disimpulkan bahwa :

1. Dalam implementasi keamanan jaringan firewall raw pada router mikrotik, menunjukan bahwa firewall raw pada router mikotik dapat mengurangi penggunaan CPU Load dan free Memory saat terjadinya serangan DDoS. Meskipun belum sepenuhnya efektif dalam menangani serangan secara keseluruhan, terutama pada skala serangan yang lebih besar.
2. Dalam pengujian Quality of service pada router mikrotik, baik saat firewall raw diaktifkan maupun tidak, tidak terlihat perbedaan yang signifikan pada parameter QoS. Hal ini menunjukkan bahwa meskipun firewall raw telah diaktifkan untuk menangani serangan DDoS, efektivitas dalam meningkatkan parameter QoS masih terbatas.

B. Saran

Berdasarkan pada hasil kesimpulan di atas, maka penulis memberikan saran sebagai berikut:

1. Penelitian dilakukan dengan skala jaringan yang kecil. Untuk penelitian lebih lanjut, disarankan untuk menguji efektifitas Firewall Raw pada skala jaringan yang lebih besar, dengan jumlah perangkat dan pengguna yang lebih banyak, untuk mendapatkan hasil yang lebih komprehensif.
2. Disarankan untuk penelitian lebih lanjut, dapat mengembangkan penelitian dengan menguji metode keamanan jaringan lainya selain firewall raw, seperti intrusion Detection System (IDS) atau Intrusion Prevention System (IPS).

4. Hasil Pengujian Dan Analisa

Tabel 8 Hasil Pengujian dan Analisa

No	Jenis Pengujian	Kriteria	Hasil	Keterangan
1	Pengujian serangan DDoS Pada	Pengujian dilakukan menggunakan aplikasi hping3 di kali linux	Serangan TCP Flood, UDP Flood, dan ICMP Flood dapat menembus router sehingga meningkatkan cpu load	Berhasil melakukan serangan

P-ISSN 1858-2680
E-ISSN 2723-4673

	Jaringan Lokal		menjadi 100% dan free memory 5.8 MiB	
2	Pengujian Serangan DDoS Pada Jaringan Internet	Pengujian dilakukan menggunakan aplikasi hping3 di kali linux	Serangan TCP Flood, UDP Flood, dan ICMP Flood dapat menembus router sehingga meningkatkan cpu load menjadi 100% dan free memory 4 MiB	Berhasil dilakukan
3	Pengujian penggunaan Sumber Daya Router Mikrotik	Pengujian ini dilakukan menggunakan Tools Resource pada aplikasi winbox	Dengan *Firewall Raw* beban *CPU* stabil di 60-70%, dan *Free Memory* meningkat menjadi 9-10 *MiB*, dan pada jaringan internet *CPU Load* dari 100% turun menjadi 5% dan *free memory* dari 5 *MiB* meningkat menjadi 8.0 *Mib*.	Firewall raw berhasil dapat menurunkan beban CPU Load dan mempertahankan free memory
4.	Pengujian Kualitas Jaringan	Pengujian parameter throughput	Pada jaringan local di peroleh sebesar 107 tanpa firewall dan 149 kb dengan firewall raw dan pada jaringan internet 32 kb tanpa firewall raw dan 128 kb dengan firewall raw	Dari nilai yang peroleh throughput dikategorikan sagat rendah berdasarkan tiphon
		Pengujian Parameter Delay	Pada jaringan local kualitas jaringan di peroleh sebesar 25.57 ms tanpa firewall raw dan 37.47 ms dengan firewall raw dan jaringan internet tanpa firewall raw 67.57 ms 26.2 ms dengan firewall	berdasarkan standarisasi TIPHON
		Pengujian Parameter Jitter	Pada jaringan local diperoleh sebesar 1.68 ms dengan firewall raw dan 1.68 ms dengan firewall raw dan jaringan internet tanpa firewall raw 1.65 ms menjadi 1.6 ms dengan firewall	Dari nilai yang di peroleh jitter pada jaringan local dan jaringan internet dikategorikan bagus berdasarkan standarisasi TIPHON
		Pengujian parameter packet loss	Pada jaringan local sebesar 0% dan jaringan internet 0%	Nilai yang diperoleh paket loss dikategorikan sangat bagus berdasarkan standarisasi TIPHON

DAFTAR PUSTAKA

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

[2] Arifin, Nofri, Yudi., et.al. 2021. *Analisa Perancangan Sistem Infromasi*. Batam: Yayasan Cendikia Mulia Mandiri. 89 hal.

[3] Anggaraini, Ayu., et.al. 2023. *Mekanisme Pembuatan Tabungan Mudharabah Pada Bank Perkreditan Rakyat Syariah (BPRS) Al Falah*. Jurnal Ilmiah Mahasiswa Perbankan Syariah Sekolah Tinggi Ekonomi dan Bisnis Syariah (STEBIS) Indo Global Mandiri, Vol.3, No.1, 183-196.

[4] BSSN (2023). Lanskap Keamanan Siber Indonesia 2023. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[5] Burhanuddin, and Najeminur. 2023. Analisis Mekanisme Pelayanan Pada Badan Pengelolaan Keuangan Dan Pendapatan Daerah (BPKPD) Kabupaten Wajo. Jurnal Manajemen dan Akuntansi, Vol.3, No.1, 108-118.

[6] Cahya, Bintang., et.al. 2023. *Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan.* Jurnal Science Informatica and Robotics, Vol.1, No.2, 63-80.

[7] Ekawati, Inna, and Irwan, D. 2021. *Implementasi Virtual Private Network Menggunakan PPTP Berbasis Mikrotik.* Jurnal Of Electrical and Electronics, Vol.9, No.1, 29-40.

[8] Fau, Alwin., et.al. 2017. Analisa Perbandingan Boyer Moore Dan Knuth Morris Pratt Dalam Pencarian Judul Buku Menerapkan Metode Perbandingan Eksponensial (Studi Kasus : Perpustakaan STMIK Budi Darma). Jurnal Times Technology Informatics & Computer System, Vol.6, No.1, 12-22.

P-ISSN 1858-2680
E-ISSN 2723-4673

[9] Fakhmi, Mhd and Glutom, Lipantri, M. 2021. *Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw*. Jurnal seminar nasional industri dan teknologi, 260-277.

[10] Harto, Muhammad, K, and Basuki, A. 2021. *Deteksi Serangan DDOS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest.* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol.5, No.4, 1329-1333.

[11] Kurniawan, Indra., et.al. 2023. Perancangan Jaringan Hotspot Di Universitas Nahdlatul Ulama Sumatera Barat Menggunakan Mikrotik Dalam Manajemen Bandwidth. Jurnal Teknik Informatika dan Sistem Informasi, Vol.1, No.1, 21- 25.

[12] Mamuriyah, Nimatul., et.al. 2024. Rancangan Sistem Keamanan Jaringan Dari Serangan DDos Menggunakan Metode Pengujian Penetrasi. Jurnal Teknologi Dan Sistem Informasi Bisnis, Vol.6, No.1, 162-167.

[13] Nasution, Wahyudi. 2024. Mekanisme Pembiayaan Mitra Guna Berkah Pns Dengan Akad Murabahah Pada Bank Bsi Kcp Panyabungan. Jurnal Perbankan Syariah Darussalam, Vol.4, No.1, 45-55.

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

[15] Sihotang, Bil, Klinton and Damanik, B.E. 2020. Implementasi Access Control List Pada Mikrotik dalam Mengamankan Koneksi Internet Koperasi Sumber Dana Mutiara. Jurnal Riset Komputer, Vol.7, No.2, 229-234.

[16]

[17] Wahyuni, and Adytia, P. 2022. Perbandingan Algoritma Machine Learning Dalam Mendeteksi Serangan DDOS. Jurnal Teknologi Informasi Komunikasi, Vol.9, No.2, 161-166.

P-ISSN 1858-2680
E-ISSN 2723-4673