JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 03, N0. 01, Tahun 2025, Hal. 48- 63, ISSN: 3031-9498 (Online)

Sistem Monitoring Serangan pada Mikrotik Berbasis Bot Telegram untuk Keamanan Jaringan yang Efektif

Perinda Putri Depani[1], Abdul Wahid[2], Muh. Syahid Nur Wahid[3]
[123]Universitas Negeri Makassar
Email : putridepani03@gmail.com

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 07, 2024

Keywords:

bot telegram, DDoS, firewall raw, MikroTik router, monitoring.

ABSTRACT

Network security systems are a very important aspect of maintaining the integrity and availability of network services. MikroTik router as one of the commonly used network devices and is vulnerable to various types of attacks, including Distributed Denial of Service (DDoS) attacks. This research uses the Experiment method. This research aims to develop an attack monitoring system on MikroTik devices by using Telegram bots as a real-time notification tool to improve responses to potential network security threats. This research utilizes a raw firewall as a solution to block DDoS attacks, which is integrated with Telegram bots to provide immediate notifications to network administrators when an attack occurs. The results of this research show that the raw firewall can block DDoS attacks, and the developed monitoring system can detect and provide notifications to telegram bots effectively and improve responses to network security threats.

Article Info

Article history:

Received September 25, 2024
Revised October 06, 2024
Accepted October 07, 2024

Keywords:

bot telegram, DDoS, firewall raw, MikroTik router, monitoring.

ABSTRACT

Sistem keamanan jaringan menjadi aspek yang sangat penting dalam menjaga integritas dan ketersediaan layanan jaringan. MikroTik router sebagai salah satu perangkat jaringan yang umum digunakan, rentan terhadap berbagai jenis serangan, termasuk serangan Distributed Denial of Service (DDoS). Penelitian ini menggunakan metode eksperimen. Penelitian ini bertujuan untuk mengembangkan sistem monitoring serangan pada perangkat MikroTik dengan menggunakan bot Telegram sebagai alat notifikasi real-time untuk meningkatkan respons terhadap potensi ancaman keamanan jaringan. Penelitian ini memanfaatkan firewall raw sebagai solusi untuk memblokir serangan DDoS, yang diintegrasikan dengan bot Telegram untuk memberikan notifikasi langsung kepada administrator jaringan ketika terjadi serangan. Hasil dari penelitian ini menunjukkan bahwa firewall raw dapat memblokir serangan DDoS sistem monitoring yang dikembangkan mampu mendeteksi dan memberikan notifikasi pada bot telegram secara efektif, serta meningkatkan respons terhadap ancaman keamanan jaringan.

Corresponding Author:

Nama penulis: Perinda Putri Depani
Universitas Negeri Makassar
Email: putridepani03@gmail.com

Pendahuluan

Sistem jaringan di Indonesia mengalami kemajuan yang pesat dalam beberapa tahun terakhir. Hal ini didorong oleh beberapa faktor yaitu peningkatan infrastruktur telekomunikasi, seperti pembangunan jaringan erat optik dan peningkatan kapasitas jaringan seluler dan bertumbuhnya kesadaran masyarakat akan pentingnya akses internet. Berdasarkan data yang diperoleh dari Kementerian Komunikasi dan Informatika (Kominfo), terdapat peningkatan sebanyak 73,7% dalam jumlah pengguna Internet di Indonesia pada tahun tertentu, naik dari angka sebelumnya sebesar 63,8% pada tahun 2018. Peningkatan ini tidak hanya mencakup penggunaan Internet yang meningkat, tetapi juga disertai dengan pertumbuhan jumlah pengguna komputer (Fahrezi et al., 2023).

Terdapat beberapa tantangan dalam keamanan jaringan yaitu hilangnya kesadaran masyarakat tentang pentingnya keamanan cyber membuat mereka rentan terhadap serangan. Selain itu, serangan cyber terus berkembang dan menjadi lebih canggih. Serangan seperti ransomware, phising, DDoS (Denial-of-service attack), dan malware menjadi semakin umum dan dapat menyebabkan kerugian finansial yang signifikan yang merupakan ancaman besar bagi keamanan jaringan di Indonesia(Siregar, 2012).

Perkembangan teknologi internet yang pesat memiliki dampak yang tidak bisa diabaikan terhadap peningkatan kasus kejahatan siber. Oleh karena itu, para pengelola jaringan komputer perlu mewaspadai jumlah serangan yang dapat dilakukan di internet oleh para peretas. Salah satu bentuk serangan yang sering terjadi dalam jaringan komputer adalah serangan DDoS. Serangan DDoS merupakan tindakan yang bertujuan untuk mencegah atau merusak kemampuan pihak yang berwenang dalam menggunakan jaringan, sistem, atau aplikasi dengan menghabiskan sumber daya seperti CPU, memori, bandwidth, dan ruang disk (Luthfansa & Rosiani, 2021).

Permasalahan dalam sistem keamanan jaringan yang dihadapi adalah terkait dengan metode monitoring yang masih bersifat manual. Pada sistem yang menggunakan metode manual, seorang administrator harus secara aktif login ke sistem secara berkala untuk memeriksa potensi serangan atau kejadian yang mencurigakan. Pendekatan ini tidak hanya memakan waktu, tetapi juga kurang efisien dalam mendeteksi serangan siber secara cepat dan akurat.

Permasalahan lain yang muncul adalah tidak adanya notifikasi secara real- time. Dalam sebuah sistem keamanan jaringan yang efektif, notifikasi real- time menjadi sangat penting untuk memberikan respon yang cepat terhadap ancaman atau serangan yang mungkin terjadi. Tanpa notifikasi real-time, waktu respon terhadap serangan dapat menjadi lambat, memberikan peluang bagi serangan untuk merusak atau mengakses data yang sensitif (Zuhdianto & Mukti, 2023).

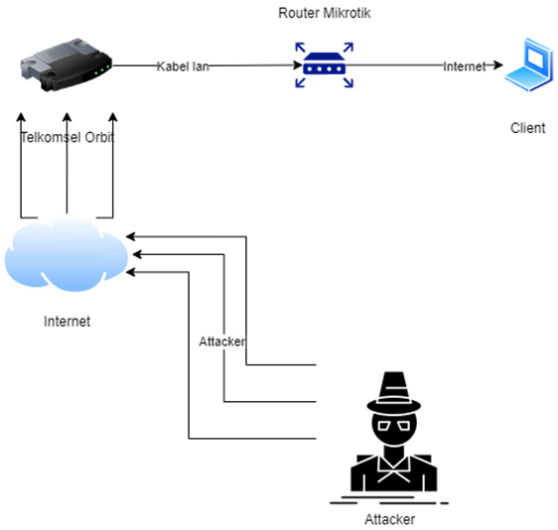
Pemilihan Telegram sebagai alat notifikasi dalam penulisan ini didasarkan pada kemampuannya untuk menyampaikan sejumlah besar pemberitahuan dari sistem keamanan. Dengan Telegram, semua pesan dan file yang diterima dapat disimpan di cloud, mengurangi beban memori pada perangkat administrator dan memfasilitasi proses pengiriman yang lebih efisien (Nurhayati, 2020). Solusi untuk mengatasi permasalahan ini dapat melibatkan implementasi sistem monitoring yang otomatis dan canggih yang dapat memberikan notifikasi secara real-time kepada administrator. Pemantauan otomatis dapat memproses dan menganalisis data dengan lebih cepat, sementara notifikasi real-time memungkinkan tindakan segera untuk merespons ancaman keamanan. Dengan demikian, organisasi dapat meningkatkan efisiensi dan efektivitas sistem keamanan jaringan mereka. Sistem monitoring yang diusulkan adalah sistem notifikasi melalui aplikasi pesan instan Telegram.

Berdasarkan latar belakang tersebut, penulisan ini bertujuan untuk mengatasi serangan DDoS yang merupakan salah satu ancaman utama dalam keamanan jaringan di Indonesia. Penulis tertarik untuk melakukan penulisan ini dengan menerapkan firewall raw sebagai solusi untuk memblokir serangan DDoS. Melalui penulisan ini, diharapkan dapat dikembangkan metode yang efektif dalam menghadapi serangan DDoS yang semakin kompleks dan merugikan. Implementasi firewall raw diharapkan dapat meningkatkan keamanan jaringan dengan meminimalkan dampak dari serangan DDoS dan menjaga kelancaran operasional sistem. Selain itu, penulisan ini juga dapat memberikan kontribusi dalam pengembangan teknologi keamanan siber di Indonesia.

Metode

1. Perancangan Sistem

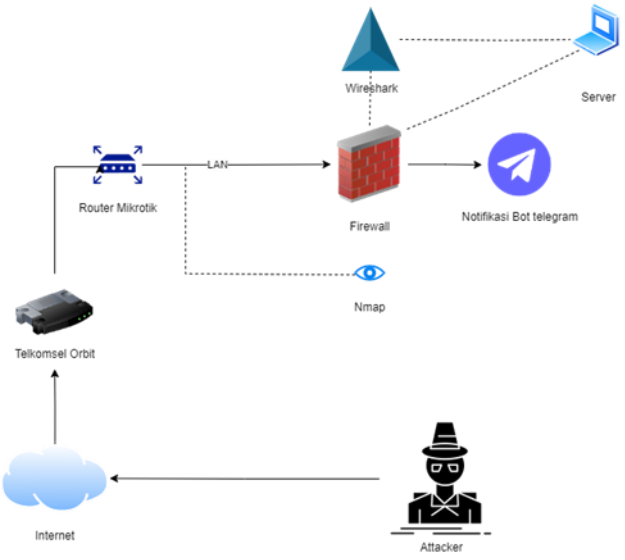
Pada penulisan ini dilakukan perancangan sistem monitoring serangan pada Mikrotik berbasis bot Telegram. Sistem ini bertujuan untuk meningkatkan keamanan jaringan dengan mendeteksi dan menindak serangan secara cepat dan efektif.



Gambar 1. Topologi Sebelum Konfigurasi

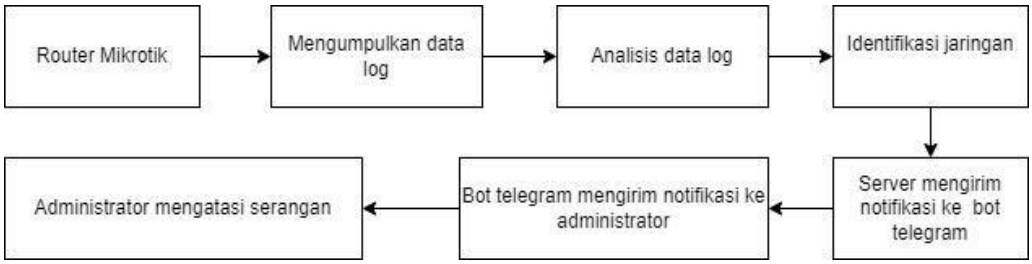
Gambar 1 menjelaskan topologi sebelum konfigurasi, pada saat terjadi serangan Attacker akan melakukan akses untuk melakukan serangan DDoS melalui internet yang terhubung kepada mikrotik mudah mengakses routerboard mikrotik. Karena pada saat mikrotik

belum konfigurasi firewall, tidak ada penghalang atau Firewall, jadi pada saat serangan DDoS, akan langsung bisa mengkakses laptop atau server client yg terhubung dengan mikrotik.



Gambar 2. Topologi Setelah Konfigurasi

Gambar 2 menjelaskan topologi jaringan sesudah konfigurasi, membuat konfigurasi Firewall untuk memblokir serangan DDoS yg dilakukan ke oleh attacker. Penulis membuat Firewal TCP, UDP, ICMP, dan pada saat terjadi serangan mikrotik akan mengirimkan berupa notifikasi ke bot telegram. Sedangkan client akan mendapatkan sebuah notifikasi bot telegram.



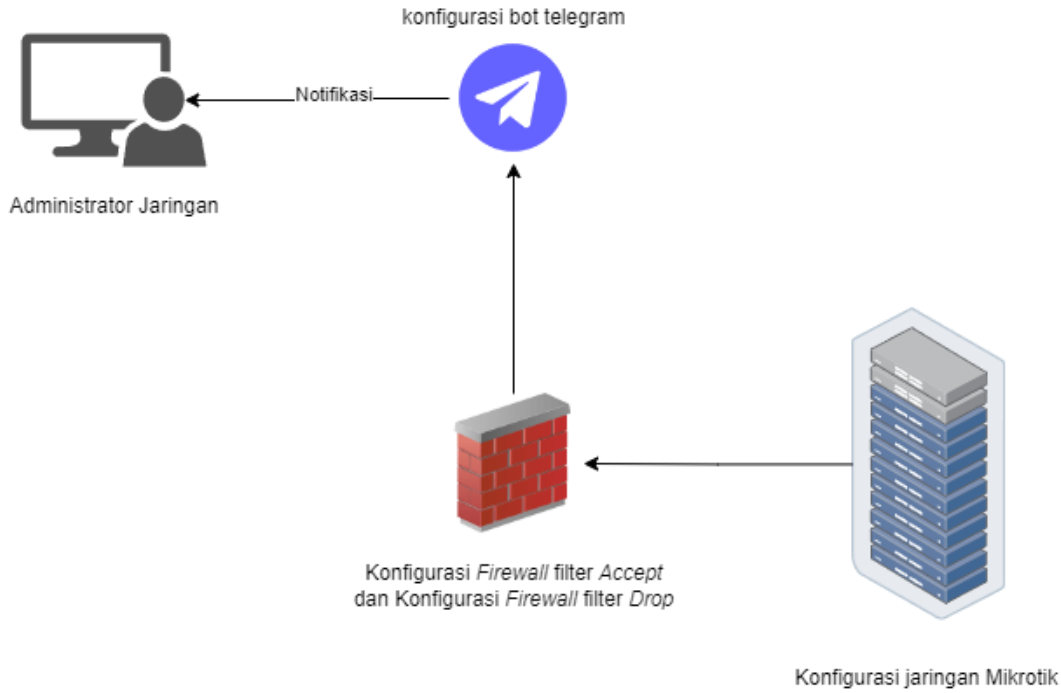
Gambar 3 Skema Sistem

Gambar 3 Router MikroTik dikonfigurasi untuk mencatat aktivitas jaringan seperti alamat IP, waktu, dan jenis lalu lintas. Data tersebut kemudian disaring untuk mendeteksi tindakan mencurigakan, seperti lonjakan trafik atau upaya login yang gagal. Setelah difilter, data yang relevan dikirim ke server melalui protokol aman seperti SSH. Di server, data log diproses untuk mengidentifikasi Pola serangan dengan menggunakan skrip atau program khusus, mungkin dengan teknologi seperti ekspresi reguler atau pembelajaran mesin. Jika ada serangan yang terdeteksi, server menentukan jenis dan tingkat keparahan serangan, dan kemudian mengirimkan notifikasi berisi informasi penting seperti jenis serangan, alamat IP sumber, dan waktu serangan ke bot Telegram melalui API Telegram. Bot Telegram kemudian menerima notifikasi, mengekstrak informasi penting, dan mengirimkannya kepada administrator jaringan melalui chat pribadi di Telegram. Administrator jaringan, yang menerima notifikasi pada perangkat mobile mereka, menganalisis informasi serangan untuk

menilai situasi dan tingkat keparahan, lalu mengambil langkah-langkah yang diperlukan untuk menangani serangan tersebut, seperti memblokir alamat IP sumber di firewall.

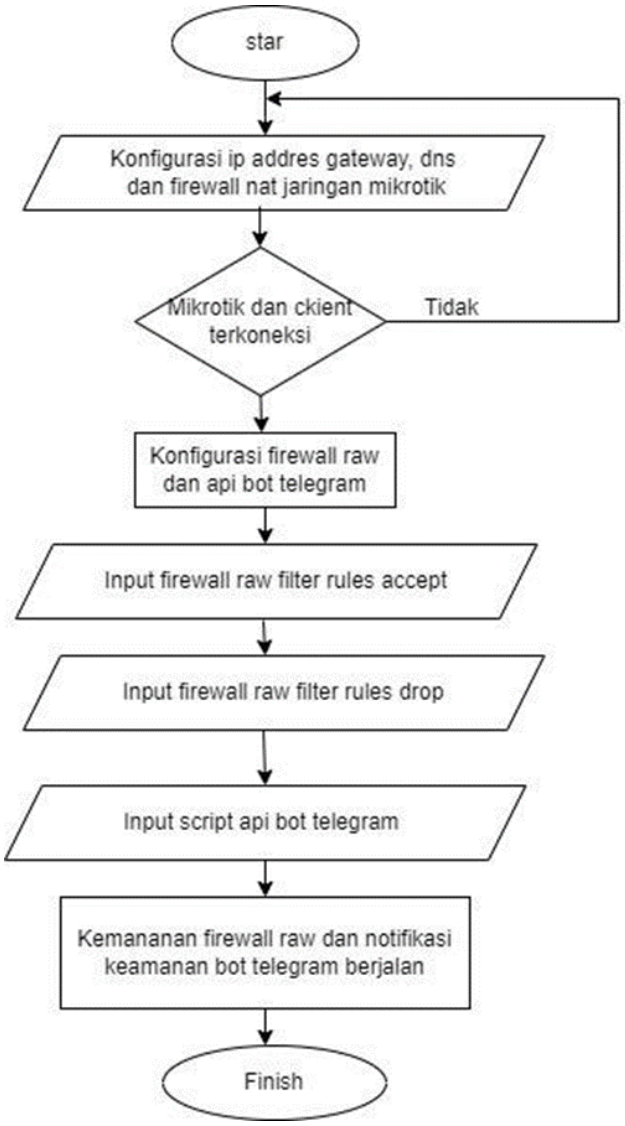
2. Struktur Implementasi

Pada tahap implementasi sistem sesuai rancangan yang telah dibuat, akan dilakukan penguraian mengenai rancangan sistem keamanan jaringan yang menggunakan firewall raw untuk melindungi dari serangan DDoS pada perangkat MikroTik. Firewall raw diimplementasikan sebagai langkah proaktif untuk melindungi jaringan dari serangan DDoS, dengan aturan yang dirancang untuk mengidentifikasi dan menanggapi serangan DDoS secara efektif. Penggunaan API bot Telegram memungkinkan administrator jaringan menerima notifikasi secara instan, memungkinkan tanggapan cepat terhadap serangan. Keseluruhan rancangan sistem bertujuan untuk meningkatkan keamanan jaringan MikroTik dan memberikan perlindungan yang optimal terhadap ancaman serangan DDoS. Pembuat telah menambahkan topologi struktur implementasi sebagai berikut:



Gambar 4. Topologi Struktur Implementasi

Tahap pertama adalah melakukan konfigurasi jaringan pada perangkat MikroTik, diikuti dengan konfigurasi firewall raw yang mencakup aturan Firewall Filter Accept dan Firewall Filter Drop. Selain itu, dilakukan juga konfigurasi API bot Telegram untuk memastikan notifikasi dapat diterima melalui bot Telegram.



Gambar 5. Flowchart Impelementasi Sistem

Gambar 5 merupakan flowchart implementasi sistem pada peneilitian ini terdapat beberapa langkah yang dapat dilakukan yaitu: langkah pertama adalah Konfigurasi IP address gateway, DNS, dan firewall NAT jaringan Mikrotik untuk memastikan bahwa router Mikrotik sudah terkonfigurasi dengan benar dan dapat terhubung ke internet. Langkah kedua konfigurasi firewall raw Langkah ini dilakukan untuk membuat aturan firewall yang akan digunakan untuk mendeteksi serangan.

Aturan firewall ini akan menentukan jenis serangan apa saja yang akan dideteksi dan bagaimana cara menanganinya. Langkah ketiga yaitu Input firewall raw filter rules accept Langkah ini dilakukan untuk menambahkan aturan firewall yang akan menerima paket data yang tidak berbahaya. Menambahkan aturan firewall yang akan menolak paket data yang berbahaya. Langkah kelima Input script API bot Telegram Langkah ini dilakukan untuk menambahkan skrip yang akan digunakan untuk mengirimkan notifikasi serangan ke Telegram. Langkah keenam Keamanan firewall raw dan notifikasi keamanan bot Telegram berjalan Langkah ini menunjukkan bahwa konfigurasi firewall raw dan API bot Telegram sudah selesai dilakukan dan sistem sudah berjalan dengan baik.

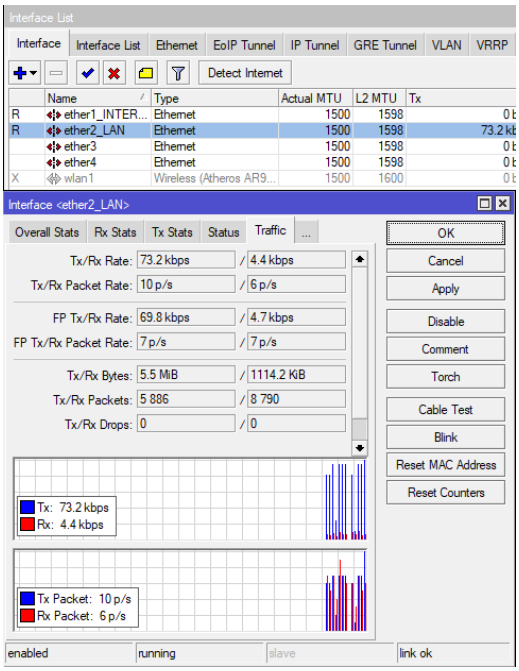
Hasil

1. Notifikasi Bot Telegram

Gambar 6. Notifikasi dari Firewall telah Mendeteksi Serangan

Gambar 6 menjelaskan Firewall telah mendeteksi penyerangan DDoS, setelah terjadi serangan DDoS Firewall akan memblokir serangan dan akan mengirimkan pesan secara singkat dan jelas, setelah firewall mendeteksi serangan DDoS, Firewall akan melangsungkan pesan kepada bot telegram dan pesan berisi tanggal dan waktu secara real-time.

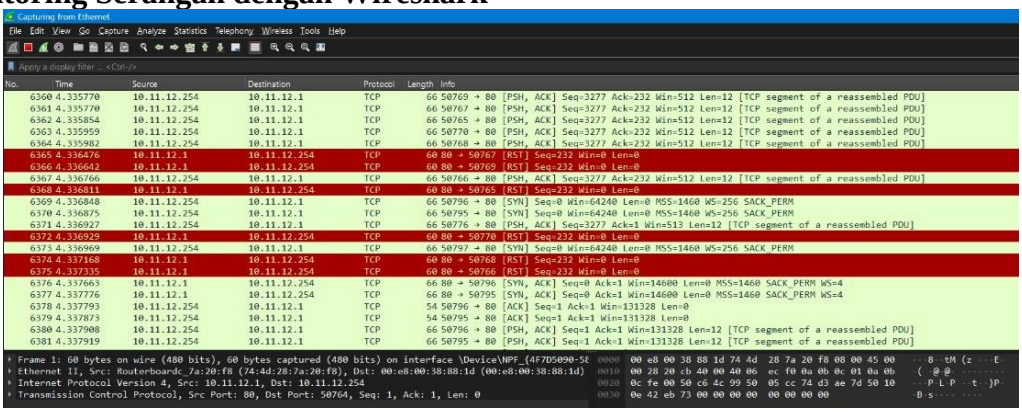
2. Trafik Monitor List



Gambar 7. Trafik Interface etehr2

Gambar 7 menjelaskan, Interface ether2 berfungsi untuk memonitor trafik pada saat waktu penyerangan dan trafik akan meningkat saat terjadi serangan DDoS, dan akan menurun pada saat telah terjadi serangan.

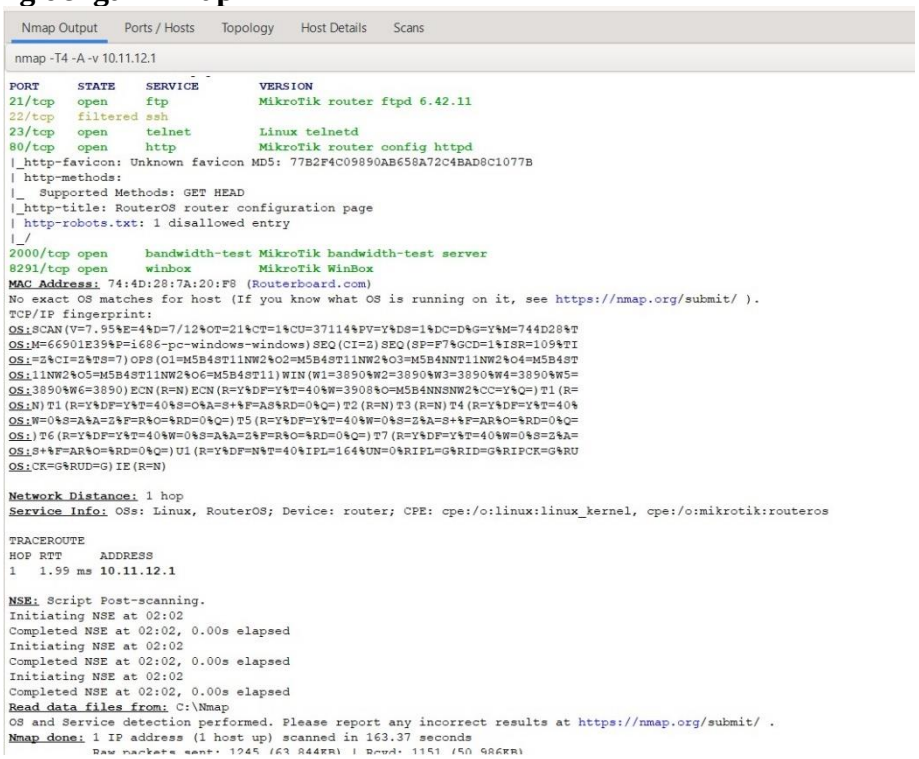
3. Monitoring Serangan dengan Wireshark



Gambar 8. Hasil Deteksi Serangan

Gambar 8 monitoring serangan DDoS melalui aplikasi Wireshark, dan aplikasi wireshark telah berhasil mendeteksi serangan dan menganalisis bahwa telah terjadi serangan DDoS pada jaringan mikrotik. Firewall pada routerboard telah berhasil mendeteksi serangan DDoS yang dilakukan terhadap IP 10.11.12.1.

4. Monitoring dengan Nmap



Gambar 9. Monitroing Nmap

Gambar 9 monitoring serangan DDoS melalui aplikasi Nmap, telah berhasil mendeteksi serangan dan menganalisis bahwa ada beberapa Port terbuka, pada saat terjadi serangan DDoS pada jaringan mikrotik. Firewall pada routerboard telah berhasil mendeteksi serangan DDoS yang dilakukan terhadap IP 10.11.12.1.

5. Pengujian Implementasi Notifikasi Bot Telegram

Tabel 1. Waktu Respon Notifikasi Bot Telegram

Alat yang digunakan Attacker	Waktu Respon	Blokir IP Attacker	Notifikasi
Loic aktif	P1: 1.12 Detik P2: 1.18 Detik P3: 1.15 Detik	YA	YA
Wireshark	P1: 1.10 Detik P2: 1.15 Detik P3: 1.11 Detik	TIDAK	YA
Nmap	P1: 30.30 Detik P2: 28.34 Detik P3: 30.13 Detik	TIDAK	YA

Tabel 1 menjelaskan ialah, ketika LOIC diaktifkan maka waktu yang akan terdeteksi dan mengirimkan sebuah notifikasi ke bot telegram dengan waktu 1.12 detik. Wireshark akan mendeteksi dengan menampilkan source IP untuk mendeteksi pada saat terjadi serangan dan tidak akan memblokir IP attacker. Namp akan mendeteksi sebuah serangan dengan menemukan sebuah IP dengan mengirimkan paket untuk menganalisisnya.

6. Pengujian Efektivitas Filtering Firewall

Tabel 2. Pengujian Waktu Notifikasi Serangan

NO	Skenario Pengujian	Waktu respon	Hasil
1	Notifikasi Serangan *DDoS*	1.21detik	Terkirim
2	Notifikasi Serangan *Scan Port TCP*	1.21 detik	Terkirim
3	Notifikasi Serangan *Scan Port UDP*	2.10 detik	Terkirim
4	Notifikasi Serangan *Scan Port ICMP*	2.30 detik	Terkirim

Tabel 4.3 pengujian ini dilakukan bertujuan untuk mengevaluasi seberapa baik mikrotik dapat mencegah serangan LOIC terhadap router mikrotik. Pada pengujian ini mensimulasikan serangan LOIC terhadap port yang dilindungi oleh firewall dan memantau respon sistem pencegahan terhadap serangan yang dilakukan. Dari peengujian yang telah dilakukan akan dievaluasi jumlah serangan yang berhasil dideteksi dan jumlah IP address attacker yang berhasil diblokir oleh firewall. Hasil dari pengujian memberikan gambaran mengenai efektivitas konfigurasi firewall dalam melindungi jaringan dari serangan LOIC.

Pengujian pertama berfokus pada monitoring deteksi serangan LOIC dengan melakukan simulasi pengujian serangan LOIC. Hasilnya menunjukkan bahwa serangan berhasil dideteksi,

menandakan bahwa firewall efektif dalam mengidentifikasi serangan LOIC. Pengujian kedua menganalisis kemampuan fireewall dalam memblokir IP addreess attacker. Hasilnya menunjukkan bahwa semua IP addreess attacker berhasil diblokir dalam waktu dua detik, yang berarti firewall mampu dengan cepat mengidentifikasi dan memblokir sumber serangan, mencegah serangan lebih lanjut. Pengujian ketiga mengukur waktu respon firewall saat mendeteksi serangan. Hasilnya menunjukkan bahwa firewall merespon dalam waktu 1 detik, menandakan kemampuan firewall untuk bereaksi secara cepat terhadap ancaman yang terdeteksi, sehingga dapat mengurangi potensi kerusakan.

7. Pengujian Kinerja Sistem Notifikasi

Tabel 3. Hasil Pengujian Kinerja Sistem Notifikasi

No	Fitur Yang Diuji	Metode Pengujian	Waktu respon	Hasil Pengujian	Hasil	
					Ya	Tidak
1	Kecepatan Pengirim Notifikasi	Mengukur waktu pengiriman notifikasi setelah serangan	P1: 1.21Detik P2: 1.15Detik P3: 1.18Detik	Notifikasi terkirim bergantung pada waktu interval dari *script* dan *Scheduler*.	Ya	-
2	Konsistensi Pengiriman Notifikasi	Menguji pengiriman notifikasi dalam berbagai kondisi	P1: 1.45Detik P2: 1.39Detik P3: 1.46Detik	Notifikasi konsisten tekirim setiap serangan.	Ya	-
3	Responsivitas dalam kondisi beban tinggi	Simulasi serangan berulang dengan intensitas tinggi	P1: 1.11Detik P2: 1.20Detik P3: 1.09Detik	Notifikasi tetap terkirim tanpa penundaan.	Ya	_

Tabel 3 Pengujian ini dilakukan bertujuan untuk mengevaluasi kinerja sistem dalam mengirimkan notifikasi melalui bot telegram setelah terjadi serangan LOIC. Dari pengujian, dilakukan serangkaian simulasi serangan dan memantau waktu respon sistem dalam mendeteksi serangan dan akan memberikan waktu dibawah 2 detik untuk mengirimkan notifikasi kepada bot telegram penulis jaringan. Hasil dari pengujian memberikan peringatan notifikasi cepat kepada penulis saat terjadi serangan LOIC.

8. Analisis Data

Pengujian ini dilakukan untuk menggapai hasil yang diharapkan, IP yang telah diatur agar bisa mengakses ke dalam server mikrotik agar orang yang tidak bertanggung jawab tidak bisa mengakses server. IP yang telah ditetapkan adalah 10.11.12.1 dan IP 10.11.12.254, selain dari IP 10.11.12.1 dan IP 10.11.12.254 tidak akan bisa mengakses ke dalam server mikrotik.

Firewall akan melakukan Blok IP jika *Firewall* tidak mengenali IP tersebut, penjelasan singkat akan dijelaskan tabel dan gambar berikut:

a. Analisis log

Tabel 4. Table IP Add Request

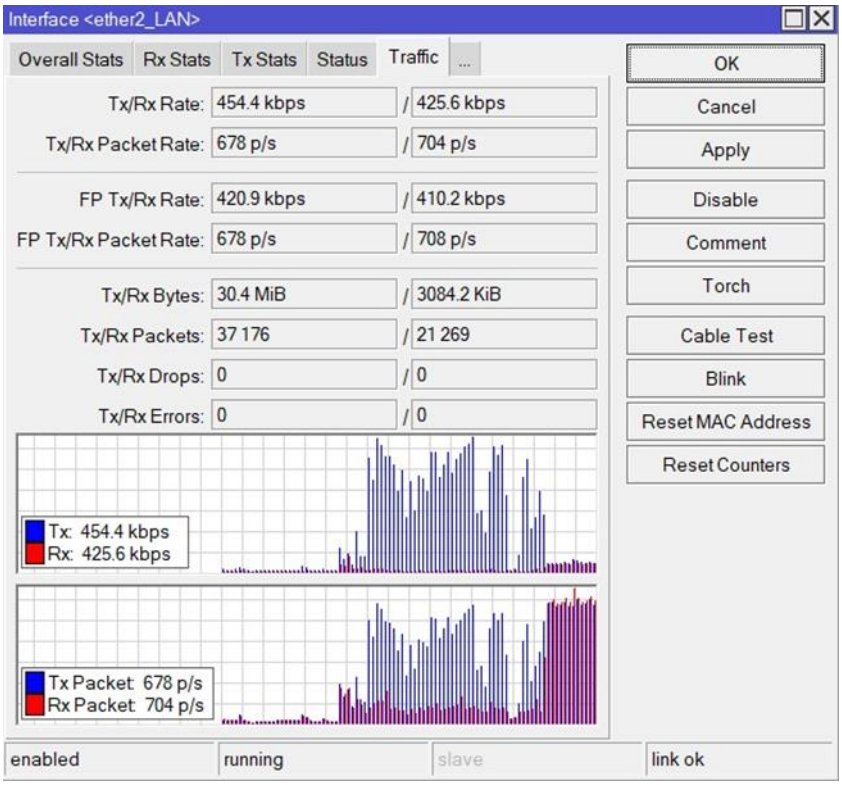
IP ADD	Request *LOIC*	Request yang di deteksi oleh mikrotik	Terblok	Percobaan login
192.168.8.1	923	923	854	100
10.11.12.1	1.094	1.094	965	136
192.168.8.245	1.588	1.588	989	167
192.168.8.255	1.968	1.968	1.450	190
192.168.8.237	2.589	2.589	1.867	145
10.11.12.1	2.477	2.477	2.236	80
192.168.8.254	3.654	3.654	2.354	120
192.168.8.293	3.065	3.065	2.154	236
10.11.12.1	4.239	4.239	3.102	110
10.11.12.254	4.567	4.567	3.303	123

Pada tabel 4 menunjukkan hasil analisis log data bagaimana sistem mendeteksi dan memblokir serangan *DDoS*, pada router mikrotik. Dalam penulisan ini, terdapat 10 percobaan yang dilakukan terhadap mikrotik. Adapun untuk menghitung persentase dari serangan sebagai berikut. (Ernawati & Sukardiyono, 2017)

$$\text{Persentase}=\frac{Jumlah\ Bagian}{Jumlah\ Keseluruhan}\ x\ 100$$

1) IP 192.168.8.1 menerima total 1,877 permintaan login. Dari jumlah tersebut 1,234 permintaan berhasil diblokir *Firewall*, yang berarti sekitar 81% dari total permintaan. Sistem berhasil mendeteksi 558 serangan. Hal ini menunjukkan bahwa *firewall* dan sistem deteksi roterboard Mikrotik bekerja dengan baik dalam memblokir dan mendeteksi serangan *DDoS*.
2) 10.11.12.1 menjadi yang paling sering diserang dengan total 3.993 permintaan. Sistem berhasil memblokir 3.447 permintaan, yang merupakan sekitar 86% dari total permintaan. Meskipun IP ini menerima jumlah serangan tinggi, tingkat keberhasilan blokirnya sangat tinggi, menunjukkan efektivitas sistem keamanan pada *Firewall* ini.
3) 10.11.12.254 menerima total 2.996 permintaan serangan. Dari jumlah tersebut, 2.475 permintaan berhasil diblokir, atau sekitar 83%. Sistem mendeteksi. IP 10.11.12.254 menunjukkan tingkat deteksi serangan yang sedikit lebih rendah dibandingkan dengan IP lainnya, tetapi tetap menunjukkan kinerja *Firewall* yang baik dalam hal blokir dan deteksi.

b. Analisis Trafik



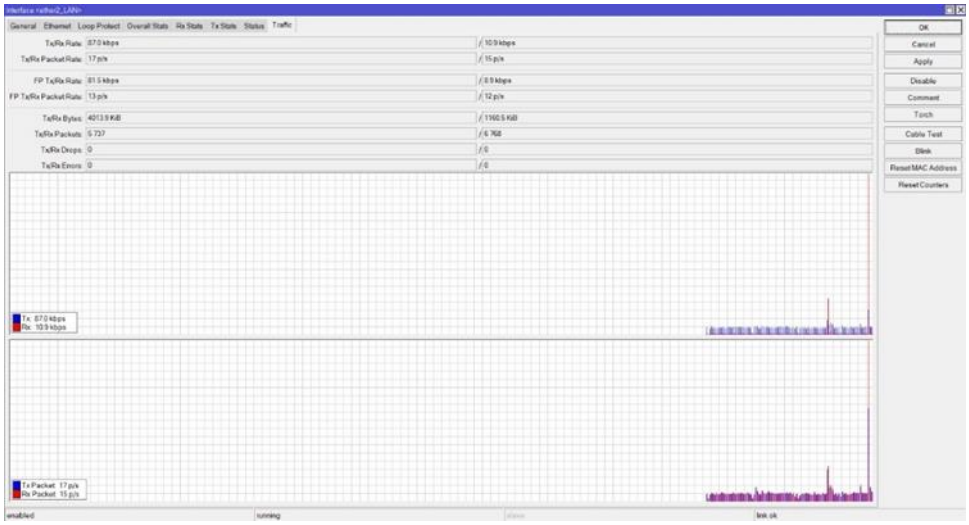
Gambar 10. Trafik Pada Saat Penyerangan

Gambar 4.32 Analisis trafik akan meningkat secara signifikan pada saat terjadi serangan *DDoS*, dan membuat CPU pada komputer akan meningkat. Batas normal *Tx* dan *Rx* Rate di angka 80 *Kbps* sampai dengan 95 *Kbps*, jika terjadi serangan *Tx* dan *Rx* akan mengalami kenaikan angka yang sangat signifikan, rata-rata dengan angka 300 *Kbps* dengan angka yang paling rendah, yang sanggup akan naik ke angka 1000 *Kbps*. Penjelasan yang detail sebagai gambar berikut:

Tabel 5. Waktu dan BandwidthTrafik Sebelum Serangan

Waktu Respon	***Bandwith***
5 Detik	71.3 *Kbps*
10 Detik	80.9 *Kbps*
15 Detik	89.4 *Kbps*
20 Deitk	93.3 *Kbps*
25 Detik	98.6 *Kbps*

Tabel 5 pada saat tidak terjadi serangan, trafik monitor tidak akan mengalami kenaikan *Bandwith* yang signifikan, rata-rata *Bandwith* dikisaran 70 *Kbps* sampai 90 *Kbps* yang trafik dalam keadaan *Bandwith* yang normal.



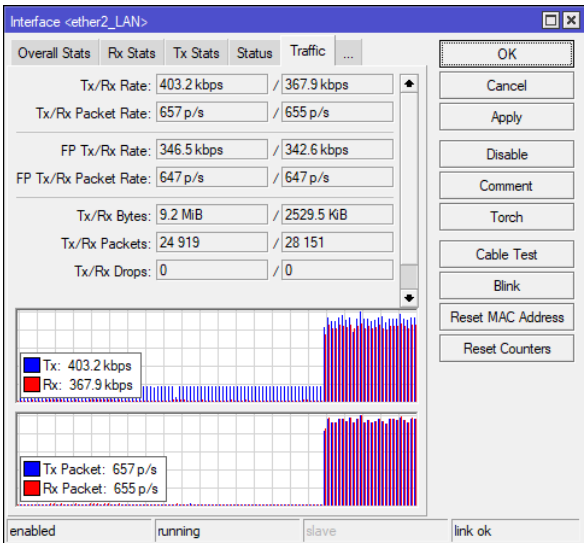
Gambar 11. Gambar Trafik dan Bandwidth Sebelum Serangan

Gambar 11 menjelaskan bahwa, gambar Trafik dan *Bandwith* sebelum serangan menjelaskan bahwa pada saat tidak terjadi serangan, trafik monitor tidak akan mengalami kenaikan *Bandwith* yang signifikan, rata-rata *Bandwith* dikisaran 70 *Kbps* sampai 90 *Kbps* yang trafik dalam keadaan *Bandwith* yang normal, seperti contoh pada table dan gambar berikut ini:

Tabel 6. Waktu dan Bandwidth Saat Terjadi Serangan

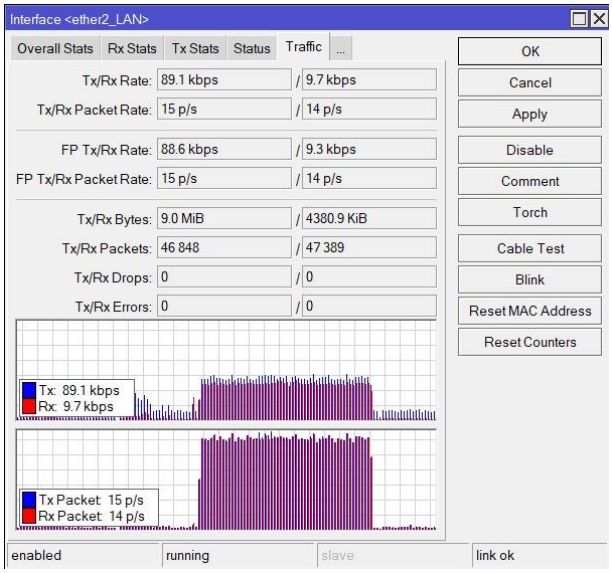
Waktu Respon	***Bandwidth***
5 Detik	1004.7 *Kbps*
10 Detik	720.1 *Kbps*
15 Detik	600.5 *Kbps*
20 Deitk	450.3 *Kbps*
25 Detik	301.6 *Kbps*

Pada saat terjadi serangan, *Bandwith* mengalami kenaikan yang sangat signifikan, artinya serangan *DDoS*, mengirim data yang sangat banyak dalam waktu beberapa detik. Rata-rata *Bandwith* akan dikisaran 1000 *Kbps* sampai dengan yang paling rendah yaitu 300 *Kbps*, *Firewall* akan berkerja semaksimal mungkin untuk menolak IP, pada saat terjadi serangan *DDoS*.



Gambar 12. Trafik Pada Saat Terjadi Serangan

Gambar 4.34 mejelaskan bahwa, trafik akan kembali normal setelah terjadi serangan DDoS. Dan Firewall bekerja sangat efisien dalam memblokir pada saat terjadi serangan DDoS, trafik monitor yang lebih jelas bisa dilihat pada gambar berikut:



Gambar 13. Trafik Setelah Penyerangan

Gambar 13 mejelaskan bahwa, trafik akan kembali normal setelah terjadi serangan *DDoS.* Dan *Firewall* bekerja sangat efisien dalam memblokir pada saat terjadi serangan *DDoS,* penyerangan *DDoS* dilakukan selama 30 detik dan trafik mencapai 1000 *Kbps,* setelah detik ke 15 *Firewall* telah bekerja sehingga menurunkan trafik ke angka 84 *Kbps.*

Pembahasan

Penelitian ini melibatkan perbandingan dengan penulisan sebelumnya dalam menangani serangan DDoS terhadap routerboard mikrotik. Penelitian sebelumnya telah mengidentifikasi kelemahan dalam sistem keamanan jaringan mikrotik dan mengusulkan solusi untuk memantau

serta mencegah serangan ini. Secara khusus, penulisan sebelumnya mungkin telah berfokus pada penggunaan teknologi yang berbeda atau persamaan yang berbeda dalam menghadapi penyerangan DDoS.

Dalam penelitian ini, terdapat perbedaan dengan membuatkan Firewall untuk memblokir serangan DDoS dengan struktur yang lebih teratur. Pendekatan ini bertujuan untuk meningkatkan keefektifan deteksi dan perlindungan terhadap serangan, dibandingkan dengan solusi yang mungkin berbeda dengan penulisan sebelumnya. Struktur Firewall yang teratur dalam routerboard mikrotik, memungkinkan identifikasi pola dalam pelacakan dan penyelidikan insiden keamanan. Penelitian ini memberikan peran firewall RAW sebagai komponen utama dalam sistem deteksi dan perlindungan. Integrasi antara routerboard mikrotik, firewall, dan analisis log diharapkan dapat memberikan perlindungan yang lebih menyeluruh dan responsif terhadap serangan DDoS. Firewall dikonfigurasi untuk memblokir serangan berdasarkan pola yang terdeteksi dalam log, meningkatkan keamanan sistem. Dengan log yang terstruktur, penulis dapat melakukan analisis terhadap pola serangan, memungkinkan deteksi dini dan respons yang lebih cepat terhadap ancaman keamanan yang muncul.

Kombinasi antara mikrotik router, firewall RAW, dan notifikasi bot telegram memberikan proteksi yang sangat baik terhadap serangan DDoS. Sistem ini dapat mendeteksi dan memblokir serangan secara efektif, serta menyimpan log untuk referensi dan analisis lebih lanjut. Penekanan pada penggunaan firewall RAW sebagai komponen dalam sistem deteksi dan monitoring melalui notifikasi bot telegram perlu perlindungan meningkatkan efektivitas deteksi serangan, dengan firewall yang mampu memblokir serangan secara real-time berdasarkan pola yang terdeteksi dalam log. Secara keseluruhan, penulisan ini tidak hanya memperkuat temuan dan rekomendasi dari penulisan sebelumnya, tetapi juga memberikan pendekatan yang menyeluruh dan terintegrasi untuk menghadapi tantangan keamanan jaringan yang semakin kompleks di era digital ini. Dengan memanfaatkan teknologi notifikasi bot telegram untuk menandakan adanya penyerangan DDoS secara Realtime dan menekankan peran firewall dalam sistem deteksi dan perlindungan, penulisan ini menawarkan solusi yang lebih efektif dan responsif terhadap serangan DDoS pada router mikrotik.

Integrasi ini diharapkan dapat memberikan perlindungan yang lebih baik dan respons yang lebih cepat terhadap ancaman keamanan, serta menyediakan data untuk analisis lebih lanjut dan peningkatan sistem keamanan di masa mendatang. Pendekatan yang lebih terstruktur dan terintegrasi ini menunjukkan kemajuan signifikan dalam bidang keamanan jaringan dan memberikan dasar yang kuat untuk penulisan dan pengembangan lebih lanjut dalam menghadapi ancaman keamanan yang semakin canggih.

Kesimpulan

Berdasarkan hasil pengujian, monitoring sistem dan alat pendeteksi serangan DDoS (Distribute Denial of Service) dengan Firewall dan notifikasi bot Telegram pada Routerboard mikrotik yang bertempat di kampus Universitas Negeri Makassar, Sulawesi Selatan. Penulis dapat menyimpulkan bahwa:

1. Melalui tahapan diantaranya, topologi menjelaskan bahwa alur rangkaian Hardware dan Software yang ingin diimplementasikan dipengujian, analisis data menjelaskan bahwa pengujian ini telah berhasil diimplementasikan. Serta pengujian Firewall, Loic (Low Orbit Ion Cannon), dan pengujian sistem telah berhasil. Sistem monitoring dan konfigurasi

menggunakan bot Telegram pada perangkat mikrotik terbukti jauh lebih efisien dalam mendeteksi serangan DDoS. Pengujian menunjukkan bahwa mengirimkan notifikasi ke bot Telegram, berhasil dengan cepat dan akurat. Memberikan notifikasi informasi lengkap kepada peneliti pada saat terjadi serangan DDoS.

2. Kinerja firewall raw, memblokir IP serangan DDoS yang akan masuk ke server dan akan memasukkan IP yang telah ditetapkan oleh penulis yaitu IP 10.11.12.1, dan efektivitas dari firewall raw tidak akan menghemat resource cpu dari pada Firewall filter. Firewall raw bisa digunakan untuk bypass IP yang tekonfigurasi ke router mikrotik, agar tidak menggunakan terlalu banyak CPU.

Adapun saran untul Penulis untuk penelitian selanjutnya yaitu mengembangkan dalam menkonfigurasikan dan memonitoring sistem pada saat penyerangan DDoS dan akan mengirimkan notifikasi kepada bot telegram yaitu:

1. Menkonfigurasi penggunaan script pada Traffic Monitor bagian threshold (bite/s) untuk mendeteksi serangan DDoS.
2. Melakukan pengembangan Firewall untuk melakukan pertahanan lebih baik, pada saat penyerangan DDoS.
3. Pengembangan cara untuk melakukan monitoring Rx Packet (p/s), pada grafik traffic monitor untuk mengirimkan notifikasi kepada bot telegram.
4. Peneliti akan memonitoring dalam penggunaan teknologi baru dan metodee lebih baik dalam mendeteksi dan mencegah serangan DDoS untuk menjaga keamanan jaringan routerboard mikrotik.
5. Penggunaan AI (Artificial Intelligence) dalam mendeteksi dan memproteksi serangan DDoS. AI dapat diterapkan dalam mendeteksi pola serangan DDoS sehingga secara otomatis AI akan membuat Rule untuk mengantipasi penyerangan DDoS.
6. Pembuat akan memvalidasi Firewall jika Serangan DDoS menyerang secara terus menerus dan akan menjadi Spam melalui notifikasi telegram.

Daftar Pustaka

Fahrezi, A., Apriliani, N., Ajijah, N., & Juardi, D. (2023). Jurnal Pendidikan dan Konseling. *Jurnal Pendidikan Dan Konseling*, *5*(1), 4093–4096.

Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal of Information Engineering and Educational Technology*, *5*(1), 34–39. https://doi.org/10.26740/jieet.v5n1.p34-39

Nurhayati, A. (2020). Monitoring Sistem Keamanan Jaringan Berbasis Telegram Bot Pada Local Area Network. *Journal of Informatics and Communication Technology (JICT)*, *1*(2), 45–53. https://doi.org/10.52661/j_ict.v1i2.41

Siregar, J. J. (2012). Analisis Explotasi Keamanan Web Denial of Service Attacks. *Handbook of Computer Networks*, *3*(9), 454–468. https://doi.org/10.1002/9781118256107.ch29

Zuhdianto, R., & Mukti, F. S. (2023). *A Clustering Optimization For Energy Efficiency In Wireless Sensor Network Using K-Means Algorithm Optimasi Proses Clustering Untuk Efisiensi Energi Pada Wireless Sensor Network Menggunakan Algoritma K-Means*. *4*(1).