Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

Network Performance Analysis and DoS Attack Mitigation Strategy on MikroTik Router for Optimal Stability

Yeni Yanti[1], Taufik Hidayat[1*], Geubrina Mahgfira[1], Nurhanif[1], Putri Nuri Pratama[1], Nadiatul Safana[1]

[1]Faculty of Engineering, Universitas Serambi Mekkah, Indonesia

*Corresponding Author: taufik.hidayat@serambimekkah.ac.id

Abstract. *The router, as a gateway in the network, plays a vital role. If its functionality is disrupted by Denial of Service (DoS) attacks, which pose a serious cyber threat and have destructive effects by overwhelming the target with large amounts of traffic, it directly impacts network performance. This research aims to analyze DoS attacks on network devices based on MikroTik routers and switches, which become targets that disrupt network traffic. These attacks lead to a significant increase in data traffic, affecting the stability and performance of the network. Through analysis using network forensic methods, this study evaluates the performance of MikroTik firewalls in mitigating DoS attacks by assessing the traffic received and rejected based on applied rules. The results show that the firewall can handle most attacks; however, some suspicious packets still bypass it. This study emphasizes the importance of enhancing security systems and mitigating DoS attacks to maintain optimal network performance in the future.*

Keywords: *mirkrotik, mitigation, denial of servis, router, firewall*

1. Introduction

Advancements in information technology today require all computer networks to demonstrate robust security system models, which are considered crucial for users seeking protection from both internal and external threats. The internet offers very open access globally and has provided invaluable contributions to its users, but this also leads to misuse that can harm the users themselves. Consequently, the responsibility lies in ensuring the security of users directly connected to the internet Various forms of threats and DoS attacks, whether direct or indirect, will impact activities occurring on the internet. Denial of Service (DoS) attacks pose a serious threat to network security, aiming to disrupt the availability of services or network resources through excessive data traffic (Elsadig, 2023). For instance, disruptions caused by DoS attacks affect bandwidth, network traffic, and applications (Yasotha & Meenakshisundaram, 2023). DoS attacks targeting bandwidth send an overwhelming number of data packets, aiming to overload and deplete bandwidth resources (Kushaeiri et al., 2024). Conversely, DoS attacks targeting network traffic flood the network with large volumes of TCP, UDP, or ICMP packets.

Internet Protocol (IP) is one of the transmission mechanisms used by the TCP/UDP protocols. where IP is unreliable, connectionless, and datagram delivery service (UDP), which results in the lack of guarantee from the IP protocol regarding the datagram (packets contained in the IP layer) sent to the destination (Amalia et al., 2022). The IP protocol attempts to ensure that the packets sent reach their destination. If during transit the packets encounter obstacles such as a broken path, congestion at the router, or the target host being down, then the TCP protocol can only inform the sender of the packet through the ICMP protocol that there has been an issue in the delivery of the IP packet

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

(Safitrah et al., 2024). Therefore, to protect against various forms of potential attacks on the network, a security system technique is required (Yunus & Lasulika, 2022; Jaya et al., 2020).

One of the efforts to prevent DoS attacks, whether through simulation or implementation, continues to evolve along with the increasing frequency of attacks on the network. Research by Hafizh et al. (2020) analyzes DoS attacks using the Wireshark simulation application to detect Netcut attacks. The results show that by placing data in the foreksi router, internet users can determine and prevent information from being misused for undesirable purposes. In addition, routers and firewall devices can also protect the network from DoS attacks (Pradhana et al., 2021). Furthermore, routers can manage connections between networks, and record the identity of data packet traffic passing through the network. Firewalls also function to protect the internal network from external threats by allowing or denying network transmission based on security rules and regulations.

Firewalls act as filters between internal and external networks by controlling based on IP addresses, ports, TCP/UDP, and other information contained in data packets. Additionally, traffic monitoring systems (MikroTik traffic monitor) are also very useful for monitoring network traffic thresholds and executing certain scripts when traffic reaches a predetermined limit (Torabi et al., 2020; Safitrah et al., 2024; Bahri, 2024). Research by Lutfi et al. (2022) used descriptive techniques to obtain data directly, the study employed flooding techniques and analyzed as well as mitigated flooding through filtering against DoS attacks. The results indicate that by implementing filtering on the MikroTik firewall, the attacks were successfully minimized, and direct mitigation was achieved by automatically dropping flooding packets, ensuring that MikroTik's performance remained stable.

Research by Fakhmi & Gultom (2021) shows that in improving the security of MikroTik routers against Syn Flood attacks using Raw Firewall, it successfully filters incoming data and tracks connections made to determine whether the connection is allowed or denied. This emphasizes that protection against DDoS attacks is not an easy task, but the use of firewall rules can help reduce the system load due to such attacks. Furthermore, ensure that the router device has sufficient CPU resources to anticipate the impact of potential DDoS attacks (Bahri, 2024).

Based on the background above, this research also conducts direct implementation to prevent DoS attacks on MikroTik router devices, so that the use of MikroTik router devices in its operational activities can be spared from material and non-material losses due to router network conditions which is down due to attacks from irresponsible individuals.

2. Method

This research utilizes network devices on routers, switches, and MikroTik devices targeting Denial of Service (DoS) attacks. These attacks are carried out by attackers (hackers) attempting to disrupt or halt network operations by flooding devices with excessive traffic. The router acts as a controller for network traffic between devices and is one of the targets of DoS attacks in this diagram. Additionally, the switch, which manages connectivity between devices within a network, also serves as a point of attack distribution. Using MikroTik devices as routers in the network makes them vulnerable to such disruptions. Collectively, these DoS attacks can cause significant disruptions to network operations by rendering services unavailable to authorized users. This figure

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

clearly illustrates how such attacks can spread to various critical devices within a network and lead to the failure of the entire network system. An analysis of the DoS attack will be conducted using forensic methods, as shown in Figure 1.

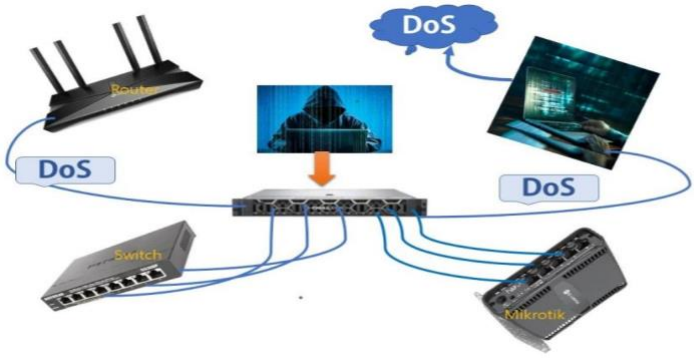

Figure 1. DoS attack activities on MikroTik router

Collectively, these DoS attacks can cause significant disruptions to network operations by making services unavailable to users. Figure 2 illustrates how such attacks can spread to various critical devices within a network, causing the entire network system to fail. The diagram shows the flow of detection and analysis of DoS attacks. This process begins by monitoring network traffic to detect suspicious activity that may indicate a DoS attack. After monitoring, the system analyzes whether a DoS attack is occurring. When an attack is detected, information about the attack is displayed along with its details. The next step is to conduct a direct forensic analysis of the ongoing attack. The goal of direct forensics is to collect evidence, identify the source of the attack, and analyze the techniques used by the attacker. This process is essential to ensure the network's security in the future. Once the forensic analysis is completed, the process is concluded to reinforce system security based on the attack's results.

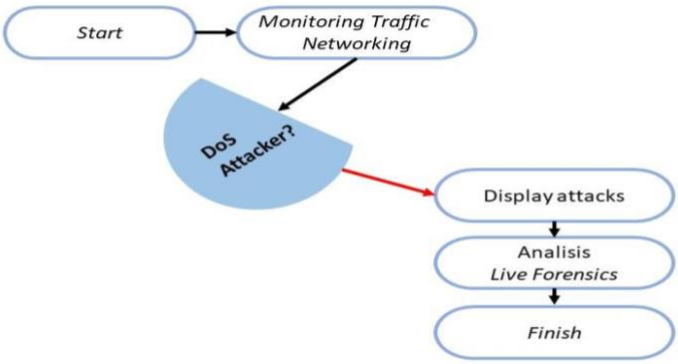

Figure 2. Denial of Service (DoS) attack detection and analysis flow

Enhancing the security of router devices can be achieved through firewall filter applications. Firewall filters aim to screen incoming data packets to prevent disruptions to the router. Meanwhile, the firewall filters incoming data and tracks established connections to determine whether they are allowed or denied. Even firewalls cannot prevent all attacks however, they can still be beneficial by making data more secure compared to having no firewall at all. Here is a scheme for enhancing the security of MikroTik routers through the use of a firewall.

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

Figure 3 illustrates the network architecture consisting of several key components: the Internet, MikroTik, firewall, and user devices such as laptops. Internet connectivity serves as an external source through the MikroTik device, which acts as a router or gateway and manages network traffic. MikroTik connects the internal network to the Internet and ensures optimal traffic management. After passing through MikroTik, data is filtered by the firewall, which acts as the primary layer of security. The firewall blocks unauthorized access, prevents threats from outside the network, and ensures that only legitimate traffic passes through. This firewall ensures that data is protected before reaching the devices. In the internal network, laptops as user devices are connected through the firewall, ensuring secure communication with the Internet. Overall, this architecture aims to ensure the security and integrity of the network by filtering traffic from the Internet before it reaches user devices.

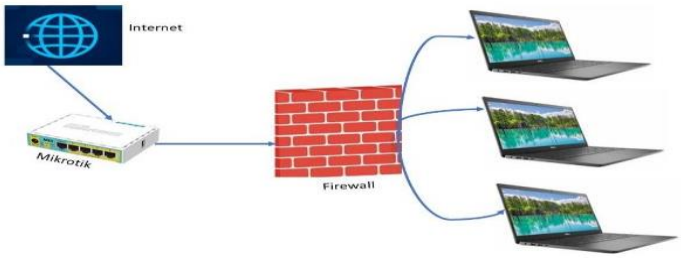

Figure 3. Networking architecture

3. Results and Discussions

The network device shown in Figure 4 has stable and optimal operating conditions. With an operating time of 13 hours and 43 minutes, this device has very low resource usage, where only 100.4 MB of a total memory of 1280 MB is used, and the processor operates at only 1% of its capacity, at a speed of 600. Internal memory is also abundant, with 190.4 MB available from a total of 1,280.8 MB, and there are no damaged memory blocks. Regarding network traffic, the device shows that the data reception speed (Rx) is much higher than the data transmission speed (Tx). The download speed reaches 5.1 Mbps, while the upload is 621.3 kbps. The packets received and sent show stable activity, with 806 packets received and 339 packets sent per second. The total data received by the device reaches 225.6 GB, while the data sent is 1.8 GB, which indicates an error in the data transmission process, showing that this device operates without interruption. Overall, the device is in very good condition, with efficient resource usage and smooth network performance. The traffic graph shows fluctuations in data activity, but there are no indications of significant problems or congestion.

Next, Figure 5 is the result of the ping command from the Windows Command Prompt to the IP address 10.10.30.1. This command uses the option to send large packets of 50,000 bytes (specified by the parameter l 50000) and ping 500,000 times (specified by n 500000). From the observations, most pings have "Request Time Out," which means the request to send data packets did not receive a response from the destination. This indicates a possible problem with the network connection, such as a lost connection or issues with the target device. However, some responses were received from the IP address 10.10.30.1, where the 50,000-byte packet was successfully sent and responded to. In one response, the time taken was 301 ms, and in another response, the response time was 452 ms. Both had a TTL (Time to Live) value of 63, indicating the number of hops (network device hops) that can still be made before the packet is considered expired. Finally, there is a connection issue that causes most packets not to be answered, although some packets

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

were sent well and received responses in relatively slow times due to a DoS attack. Thus, this results in network instability or problems with the network device handling the packets.

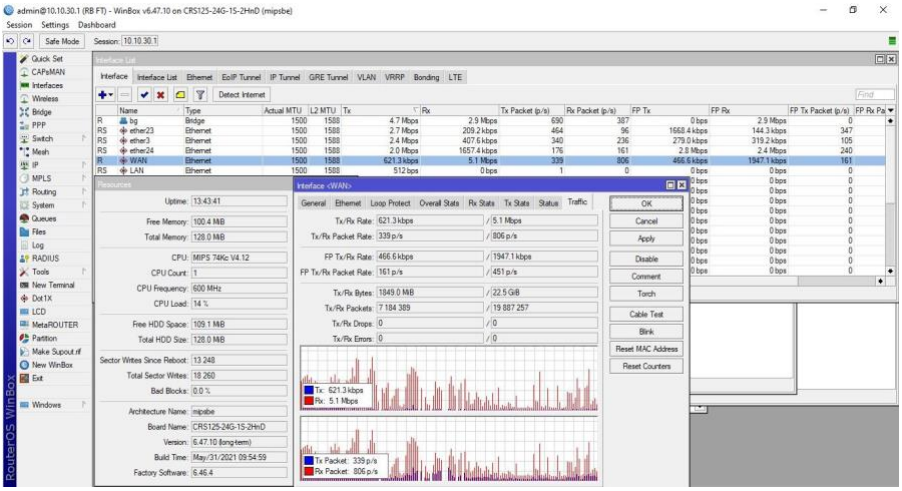

Figure 4. Initial data collection results

Next, this study also produces network traffic graph values in terms of Tx packets (transmitting packets) and Rx packets (receiving packets) measured in packets per second (p/s). This data can be seen as a continuation of previous information about network performance. Tx Packets: The transmission rate appears to be 1901 p/s, represented by the blue color in the graph. Additionally, the output from the network device is 1,901 packets per second. Rx Packets: The reception rate is significantly higher at 5273 p/s, indicated by the red color in the graph, showing that the device receives packets at a rate of 5273 packets per second. Visually, the graph indicates a significant increase in traffic, particularly in packet reception (Rx), with a clear peak in activity visible at the bottom of the graph. An increase in network activity during this period may be attributed to higher usage, user activities, or larger data transfers on the network. When combined with previous data indicating some connection timeouts, this analysis suggests that the network is handling high traffic, which could result in packet loss or unreceived responses, as indicated by earlier ping tests. This dense traffic might be one of the causes of the network instability mentioned earlier.

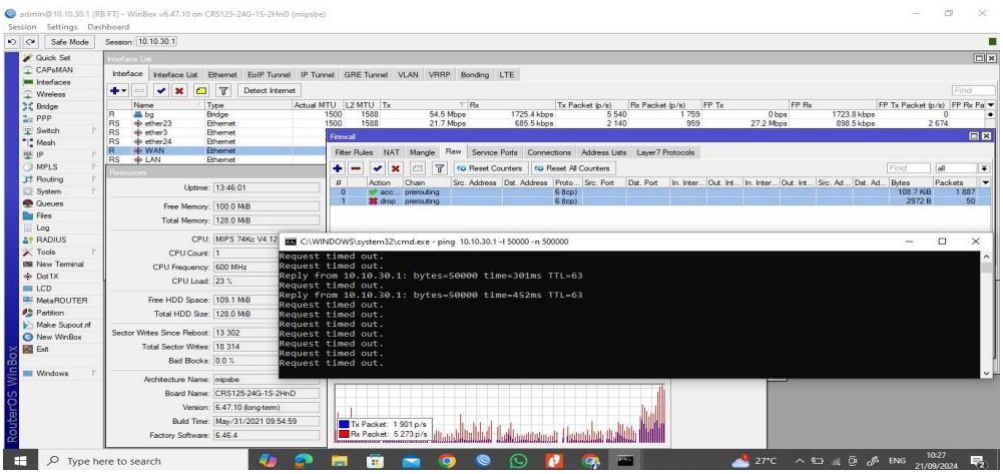

Figure 5. Result simulation of DoS

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

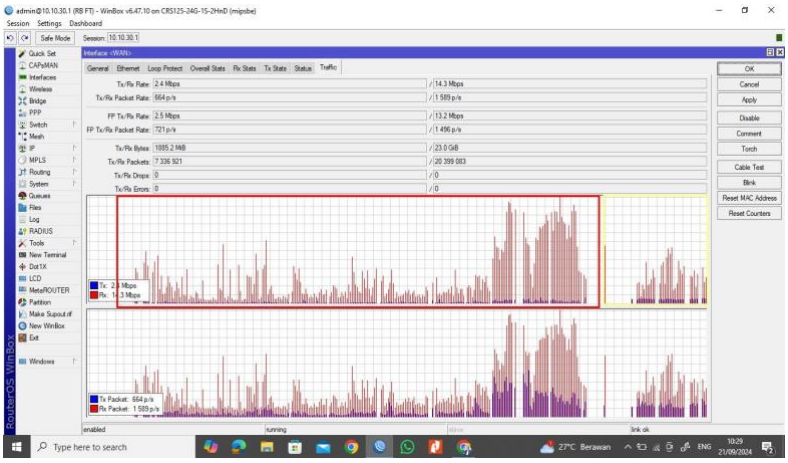

Figure 6. Traffic data of DoS

Figure 6 shows the results of network usage graphs, with two panels displaying data traffic information in the form of bar charts. In the upper panel, there are two color indicators: pink for Tx (transmit), reflecting the amount of data sent, and purple for Rx (receive), indicating the amount of data received. Tx fluctuates around 2 Mbps while Rx is approximately 1.3 Mbps, indicating significant fluctuations in network traffic. During the measurement period, several up-and-down patterns are observed, reflecting varied network activity, with notable peaks, especially between the middle and end of the period. This may reflect periods of increased data usage. To the right, there is a red-framed area that likely indicates important moments or specific events that occurred on the network during that time. In the lower panel, the graph shows a similar pattern, but in packets per second (p/s), with Tx reaching around 664 p/s and Rx approaching 1589 p/s. As in the upper panel, we observe several activity peaks with a considerable increase in both indicators, reflecting a rapid rise in the volume of packets sent and received during specific periods. Overall, this graph illustrates fluctuations in network traffic with several periods of high activity. This data can be used to analyze network performance or identify data usage patterns over a specific timeframe.

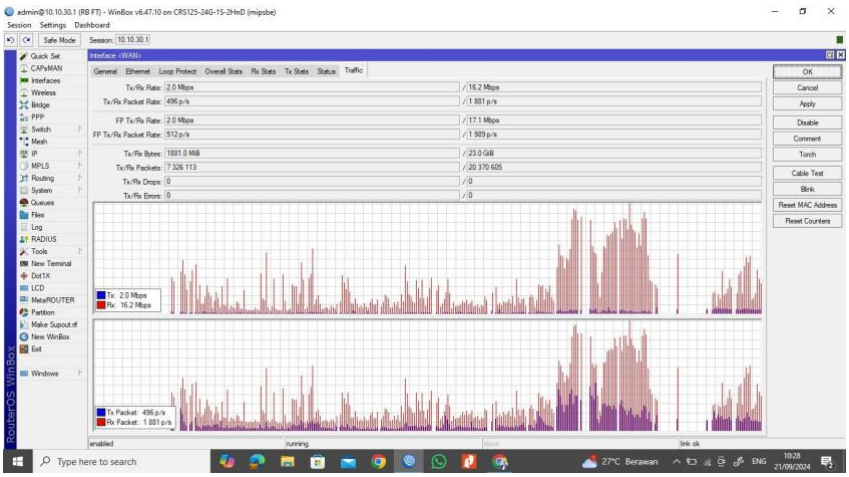

Figure 7. Result data density

The results in Figure 7 display the network usage graph with two panels illustrating data traffic. As seen in the previous Figure 3, there are two colors indicating network

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

activity: pink for Tx (transmit), representing sent data, and purple for Rx (receive), representing received data. In the upper panel, the Tx rate is around 2.0 Mbps, while Rx shows a higher value of approximately 16.2 Mbps. This indicates that the amount of data received is significantly greater than that sent. The graph pattern reveals traffic fluctuations with several significant activity spikes, especially between the middle and lower parts of the graph, where data traffic peaks, reflecting a notable increase in network activity at that time. In the lower panel, the graph displays traffic in packets per second (p/s) (Figure 8).

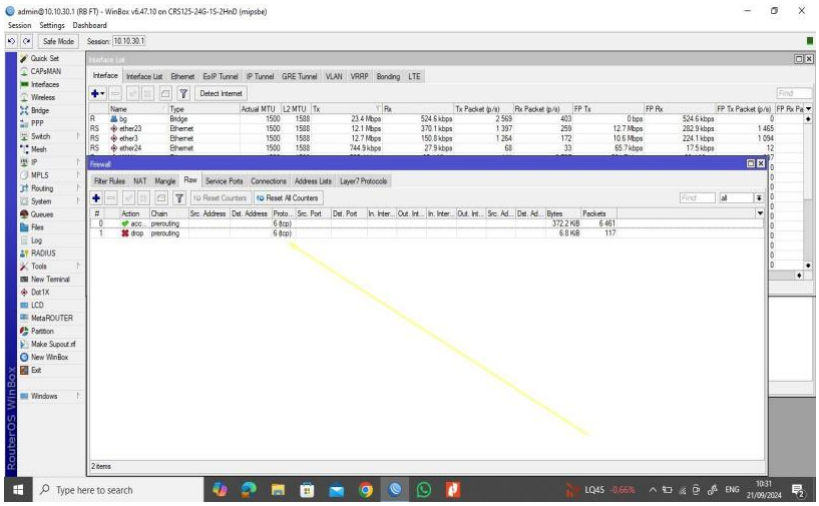

Figure 8. Data detection of DoS

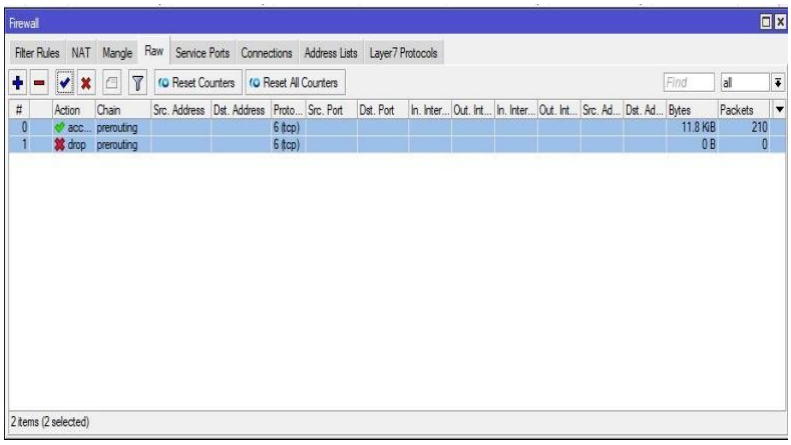

Figure 9. Result of data filter

The Tx Packet result reaches 496 p/s, while the Rx Packet reaches 1881 p/s, indicating that the volume of packets received is much higher than the packets sent. The graphic pattern of this panel is similar to the upper panel, where we see a significant increase in network activity from the middle to the end, reflecting a peak data traffic period. Overall, this graph shows a fluctuating network usage pattern but indicates a significant increase at certain times. This may indicate specific activities or events that affect network performance. Further analysis of these patterns can help to understand overall network performance and identify potential issues or the need for greater capacity during peak periods. Figure 9 shows the results of the MikroTik firewall configuration to mitigate DoS attacks. Based on the displayed data, two firewall rules are used to regulate

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

network traffic, in the acceptance and cancellation system. The first rule uses an accepted action in pre-routing, meaning that all TCP packets entering the initial stage will be accepted by the firewall before being forwarded for further processing. Based on the data, the firewall successfully filters that original traffic or from trusted sources is accepted and processed by the network, receiving as many as 210 packets with a total volume of 11.8 KB to block suspicious TCP packets or those considered part of a DoS attack. This firewall configuration effectively mitigates DoS attacks, where the original traffic is accepted through the acceptance rule, while the drop rule is set to handle suspicious traffic.

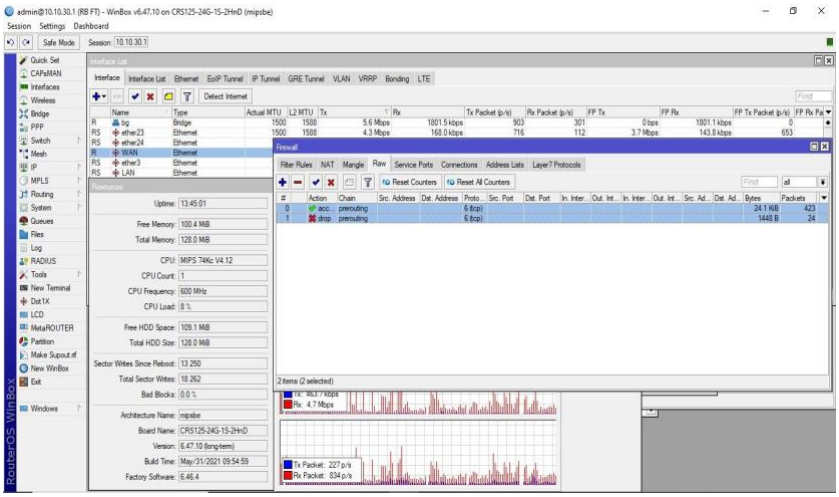

Figure 10. Result of mitigation DDoS attack

The final test results in Figure 10 display the network traffic graph, showing the statistics for received (Rx) and sent (Tx) data on the MikroTik. Further analysis reveals that the received traffic (Rx), marked in red, averages 4.7 Mbps, with considerable variation reflecting periodic increases in incoming data. In contrast, the sent traffic (Tx), indicated in blue, has a lower value of approximately 463.7 Kbps, with smaller fluctuations. In the graph below, the average packets (Tx Packet) are 227 packets per second (p/s), which tends to be stable but is significantly lower than the average received packets (Rx Packet) at 834 p/s, indicating a higher density of incoming traffic. In the context of DoS mitigation, high incoming traffic compared to outgoing traffic can serve as an early indicator of potential DoS attacks, especially if this increase occurs over a short time frame. DoS attacks are typically characterized by a much higher flow of incoming data packets compared to outgoing packets, as seen with the Rx traffic at 4.7 Mbps while Tx is only 463.7 Kbps. Additionally, there is a significant discrepancy between the number of packets received and sent, with 834 packets/s received compared to only 227 packets/s sent. This result does not suggest a balance, which could indicate a Distributed Denial of Service (DDoS) attack, where many incoming packets do not receive a response from the system server due to either overload or packet blocking. From the previous analysis, the firewall was configured with acceptance rules and was left to handle TCP traffic. However, this graph indicates that a large volume of traffic is being received, yet no packets are effectively blocked by drop rules. This suggests that the received packets do not meet the criteria for being blocked by the firewall rules, despite the very high volume, thereby increasing the likelihood of threats that require additional alerts.

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

4. Conclusions

The network devices in this study demonstrated stable and efficient performance, with the data reception speed (Rx) being higher than the transmission speed (Tx), indicating optimal traffic management. During the Denial of Service (DoS) attack, a significant traffic spike occurred. Most ping requests did not receive responses, indicating a consistent connection disruption characteristic of such attacks. Although the MikroTik firewall successfully filtered most of the traffic, some suspicious packets from the DoS attack still passed through. The performance graph (Figure 7) shows significant fluctuations and high activity that could potentially lead to instability. Therefore, this research successfully enhanced mitigation strategies using firewall filters and improved network capacity to maintain stability during traffic spikes.

5. Acknowledgments

The author would like to thank RISTEKDIKTI for supporting this research financially and also Universitas Serambi Mekkah (USM) for their support and assistance that helped this study proceed smoothly. Special thanks also to the research team for their collaboration.

6. References

Amalia, E. R., Nurheki, Saputra, R., Ramadhana, C., & Yossy, E. H. (2022). Computer network design and implementation using load balancing technique with per connection classifier (PCC) method based on MikroTik router. *Procedia Computer Science*, *216*, 103–111. doi:10.1016/j.procs.2022.12.116

Bahri, S. (2024). Mengamankan Perangkat Jaringan dari Serangan DDoS Menggunakan Fitur Firewall-RAW di Router MikroTik, *06*(01), 1–6. Retrieved from https://ejournal.ust.ac.id/index.php/KAKIFIKOM/article/view/3589

Elsadig, M. A. (2023). Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach. *IEEE Access*, *11*(August), 83537–83552. doi:10.1109/ACCESS.2023.3303113

Fakhmi, M, & Gultom, L. M. (2021). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw. *Seminar Nasional Industri dan Teknologi (SNIT)*, 260–277.

Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi dan Komputer*, *10*(2), 111. doi:10.22441/incomtech.v10i2.8757

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi dan Teknologi*, *2*, 115–123. doi:10.37034/jsisfotek.v2i4.32

Kushaeiri, F. A., Muhyidin, Y., Singasatia, D., Teknik, F., Tinggi, S., Wastukancana, T., & Barat, J. (2024). Implementasi pencegahan serangan ddos pada router, *2*, 229–244.

Lutfi, S., Khairan, A., Muin, Y., & Salmin, M. (2022). Optimal Filter Assignment Policy Against Distributed Denial of Service Attack on Router Mikrotik. *MATEC Web of Conferences*, *372*, 04008. doi:10.1051/matecconf/202237204008

Proceeding of ICMR 7(2), 241-250 DOI: https://doi.org/10.32672/picmr.v7i2.3056

Pradhana, I., Riadi, I., & Prayudi, Y. (2021). Forensik Router untuk Mendeteksi Flooding Attack Menggunakan Metode Live Forensic. *JRST (Jurnal Riset Sains Dan Teknologi)*, *5*(1), 31. doi:10.30595/jrst.v5i1.7662

Safitrah, T., Sinaga, A. B. G., Alghifari, M., & Neyman, S. N. (2024). Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest. *Journal of Technology and System Information*, *1*(4), 11. doi:10.47134/jtsi.v1i4.2663

Torabi, S., Bou-Harb, E., Assi, C., & Debbabi, M. (2020). A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. *Forensic Science International: Digital Investigation*, *32*, 300922. doi:10.1016/j.fsidi.2020.300922

Yasotha, K., & Meenakshisundaram, K. (2023). Machine Learning-Based Intrusion Detection for Mitigating Denial of Service Attacks in Wireless Sensor Networks. *International Conference on Self Sustainable Artificial Intelligence Systems, ICSSAS 2023 - Proceedings*, (Icssas), 1216–1221. doi:10.1109/ICSSAS57918.2023.10331721

Yunus, W., & Lasulika, M. E. (2022). Security System Analysis against Flood Attacks Using TCP, UDP, and ICMP Protocols on Mikrotik Routers. *International Journal of Advances in Data and Information Systems*, *3*(1), 11–19. doi:10.25008/ijadis.v3i1.1231