International Journal of Computer Sciences and Mathematics Engineering
Journal homepage: www.ijecom.org

Network Security Implementation From Ddos Attacks With Mikrotik Routers

Wirda Fitriani[1], Fachrid Wadly[2], Zuhri Ramadhan[3]
Computer Engineering Study Program, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

Article Info

Article history:

Accepted Sep 27, 2024
Revised Sep 29, 2024
Accepted Oct 01, 2024

Keywords:

Mikrotik
DDoS
Network

ABSTRACT

Cyber attacks are increasing and becoming one of the problems in the IT world. An example of the type of cyber attack used is the DDoS attack technique. Distributed Denial of Service (DDoS) attacks are one of the most frequent attacks on websites, networks, routers, and servers. Servers and network devices such as Mikrotik can also be targets of attacks. As a result, it will interfere with the organization's operational activities and cause material and non-material losses. DDoS is done to flood the target with packets sent to the target continuously. MikroTik Router is a type of router that has complete features to support network security such as firewalls. The firewall will filter the data received and track the connections made to determine whether the connection is allowed or denied. Efforts to prevent attacks are necessary with a security system. In addition, improving router security in terms of software by using Firewall Filter and Firewall Raw has proven to be effective in preventing attacks.

Corresponding Author:

Wirda Fitriani,
Computer Engineering Study Program, Faculty of Science and Technology, Panca Budi Development University, Medan, Indonesia.
Email: wirda@pancabudi.ac.id

1. INTRODUCTION

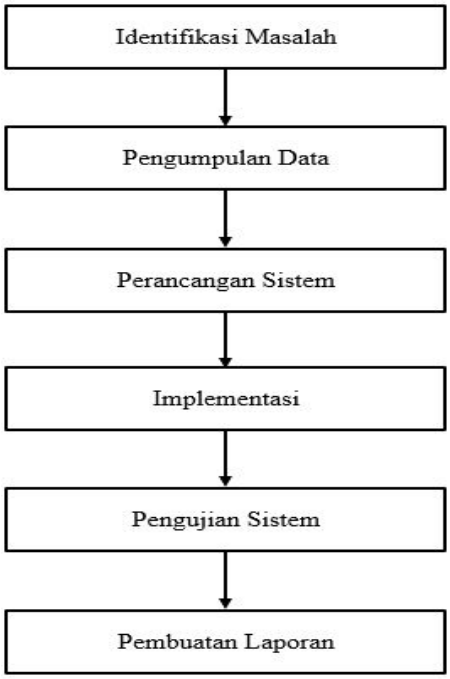
To manage a network, a tool called a router is needed. A router is a tool that uses the Linux Base operating system as a Network Router that can connect two or more different computer networks[1]. The performance measure of the router is essential for adequate user capacity with a large amount of data transmission. If a network transfers a large amount of data, there will be data flooding through Internet Protocol (IP) addresses or mac addresses[2]. This makes many hackers make Routers the main target of attacks because Routers are important devices in a network. Not only the positive side is noticed, but there is also a negative side of the development of the internet[3]. One of them is by hacking or attacking the website website which is carried out by irresponsible people. They use the internet to do vandalism against a website. In addition, usually the thing that is done by attacking network devices is a router[4]. Usually the attack overloads the router and also makes the website inaccessible. This attack technique known as DoS (Denial of Service) and DDoS (Distributed Denial of Service) is an attack carried out individually using a computer machine that is used as an attacker's medium by sending a large number of packets to the target[5].

E-ISSN 2962-4274

One of the subjects that will be the subject is about DDoS[6]. DDoS is an act that makes the server that hosts the website or application on the network unavailable to users, usually by suspending the service of a host connected to the Internet[7]. The ease of finding DDoS applications on the internet allows a person to do DDoS with the program he downloads to a desired network[4].

2. RESEARCH METHOD

In completing this final project, the author obtained data using several stages as follows:



Picture. 1 Research Flow

It can be described as follows:

a. Problem Identification
   In order to carry out the research, researchers will analyze in depth ways to deal with these attacks by utilizing raw firewall technology. The study includes strategic measures to improve protection and minimize the risk of syn flood attacks on MikroTik routers, with a focus on implementing effective and efficient raw firewall configurations[8]
b. Data Collection
   Collect data on network protection. A method of collecting data from data sources is needed to inform the problems related to this final project.
c. System Planning
   The design carried out is a network setting using a mikrotik routerboard in accordance with the topology that has been designed. The next stage of design is to set *firewall* on the mikrotik routerboard to protect the existing network on the server from attacks *Son Flood*. Then conduct a test by attacking using *Son Flood* on a mikrotic routerboard. *SYN Flood* is a form of DDoS attack in which an attacker sends a request *SYN* to the target machine with the goal of consuming server resources, thus flooding the existing connection limits. If the attacker manages to reach the connection limit, other users will not be able to connect to the server because the connection is already fully charged. Basically, when a computer connects to a server, there is a TCP connection between the client and the server, and information is exchanged as is generally the case[9].

E-ISSN 2962-4274

1. The client requests a connection to the server by sending a SYN (Synchronize) code to the server.
2. The server recognizes or acknowledges this request by sending the SYN-ACK code back to the client.
3. The client responds back by sending an ACK code and as a result a connection is established between the client and the server.

d. Implementation
The attack scheme used in this test is using the Metasploit Framework on the Kali Linux operating system. In this process, the Metasploit Framework will launch a Syn Flood attack directly on the target network of the attacked Router. By entering the target IP and the port on which the attack will be carried out. If the attack manages to penetrate the security system on the router, the attack is successful. If not, then repeat the same process, which is by entering the ip address and port of the target to be attacked.

e. System Testing
The step to handle the attack is to use the Raw Firewall as a security system applied in preventing the occurrence of Syn Flood attacks. Raw Firewall will examine the data received and track the connections made to determine whether the connection is allowed or denied. Rejected data is data sent by ports that have been blocked from accessing by the Raw Firewall. Then the firewall will block the unauthorized IP address if it tries to make a request. Data that is allowed to enter the network is data sent by ports that are not blocked by the Raw Firewall.

f. Report Creation
The report is in the form of test results from the final project/network protection research against DDoS attacks using this mikrotik router.

3. RESULTS AND DISCUSSIONS

Before starting a series of tests, the first step to take is to configure the Router using *the winbox* app to connect to the internet. In addition, it is very important to apply the pre-designed design carefully.

a. Syn Flood attacks on the network.

To conduct an initial analysis of the router, whether it is experiencing a DDoS attack or still in normal condition, monitoring can be carried out using various menus available on WinBox[10]. These menus include the Trafic, Torch, and Resources menus. The Traffic Menu is a tool used to monitor various parameters on the Router over time and organize the collected data in the form of graphs. On this graph, there are categories Tx (Transmitted Rate) and Rx (Received Rate). Tx indicates the amount of data that exits the Router through the interface, while Rx reflects the amount of data received or enters the Router through the interface.

Meanwhile, the Torch menu is a real-time traffic monitoring tool used to monitor traffic that will pass through an interface, traffic monitoring can be done based on protocol, source IP address, destination IP address, and port number. By using this feature, it is easy to get information about the traffic that occurs, such as the IP address involved, the destination of the traffic with the port used, the protocol used, and the amount of data received (Rx) and sent (Tx)[11].

In addition, there is a Resources menu that functions to provide detailed information about the system used on MikroTik, including the operating system version, hardware model, CPU load used, HDD and memory storage capacity, and other very important information. This menu provides a view of the condition of the Router before the attack occurred, so that it can see what the normal state was before the incident occurred. View before the attack[12].

E-ISSN 2962-4274

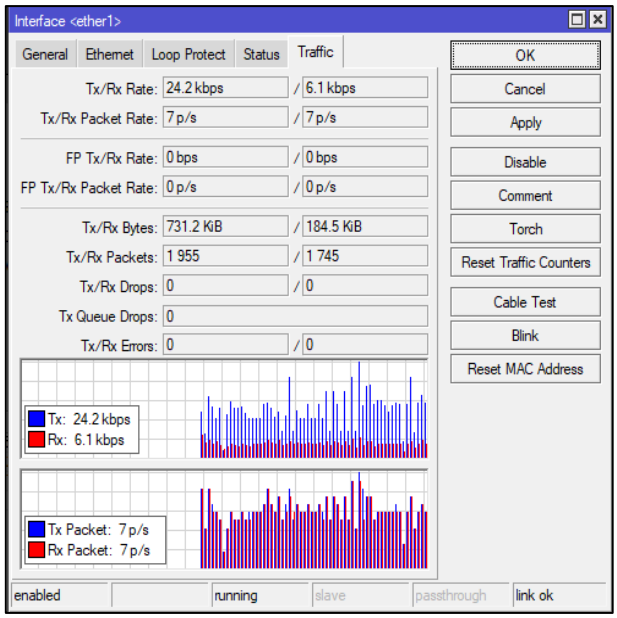
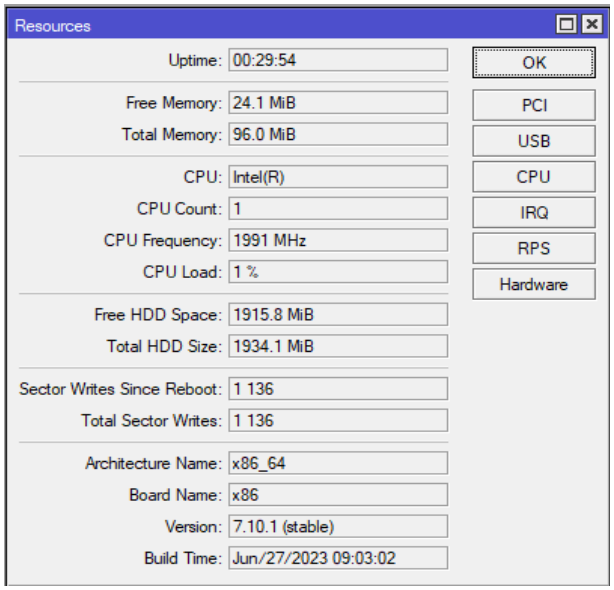


Figure 2. Traffic View Before an Attack
Source : Researcher 2024

From the image displayed, it can be observed on the Traffic menu that the graph shows that the condition of the data entering the router is in a normal state and there have been no attacks that affect network traffic on the router. The graph shows the Tx/Rx Rate values of 24.2 kbps and 6.1 kbps, as well as the Tx/Rx Packet values of 7 p/s. This indicates that communication between the client and the router is running normally. Furthermore, on the Torch menu used to monitor traffic flow, it can be seen that the condition is also in a normal state. There was no indication of any disruption or attack on the monitored traffic[13].

In the resource menu, it can be seen that the Cpu Load percentage is 1% and the Free Memory is 24.1 MiB. Both values have not changed significantly because there have been no DoS attack transactions that can affect the performance or load on the router network. This can be seen in the image shown. Overall, from the images presented, the router's condition looks normal and there are no signs of a DoS attack having occurred, which could interfere with the router's network performance[14].

E-ISSN 2962-4274



Picture. 3 Mikrotik Resources Display
Source : Researcher 2024

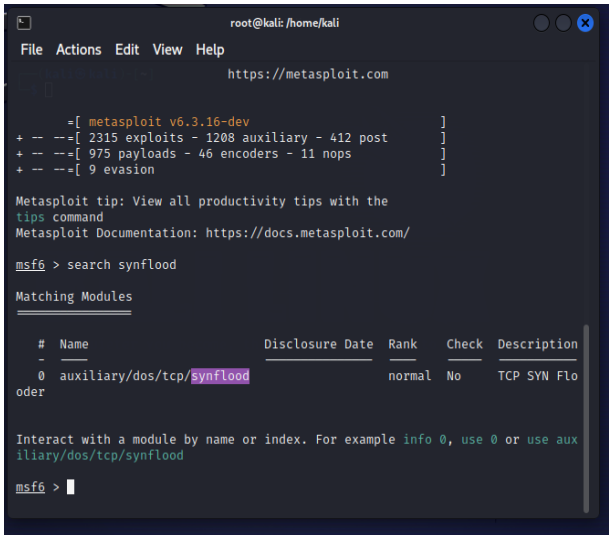
The testing process is carried out using *the Metasploit Framework* on the windows operating system. In this process, *the Metasploit Framework* will carry out *a Syn Flood* attack directly on the targeted Router network. Here are the steps taken to execute the attack

1. Running *the Metasploit framework*.
   The initial process is to run the metasploit framework by using the *postgresql start service* command to run the postgresql database on metasploit and the msfconsole command to run the metasploit framework, as shown in the following image.

Fig. 4 View Running *Metasploit*
Source : Researcher 2024

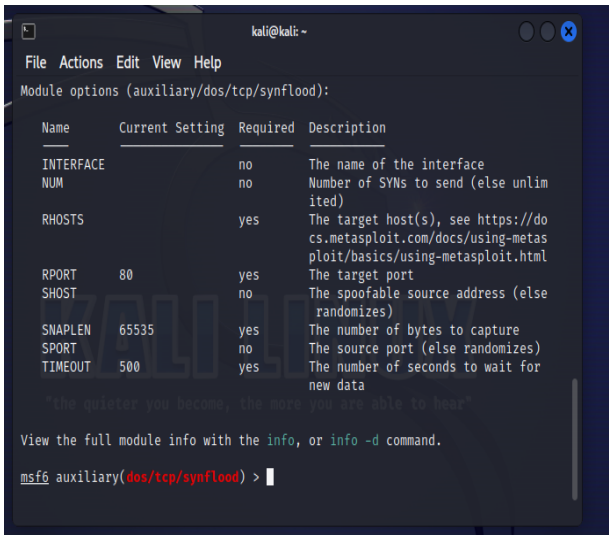
E-ISSN 2962-4274

2. Searching *for Modules*
The next step is to find the location of the *syn flood module* in the *metaslpoit* by using *the search synflood* command, and the use command to determine the module used. As seen in the following figure. This command is used.



Picture. 5 Searching Module Display
Source : Researcher 2024

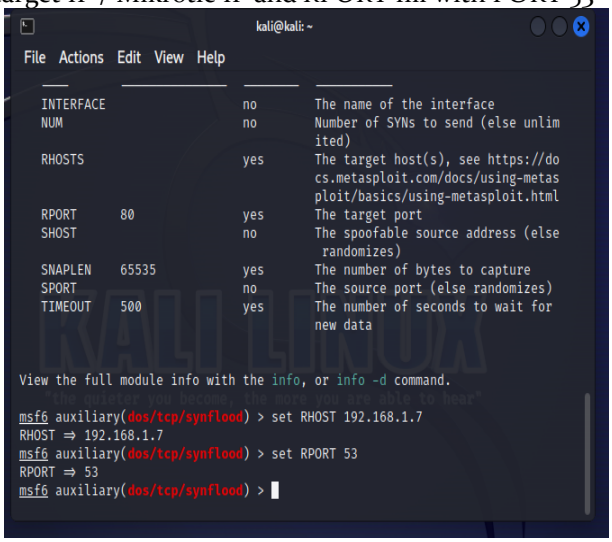
3. View options on Modules
To see the options of *available modules* or *exploits*, we can use the *show options* command, we can use the entire menu provided. But in this test, the author only uses *RHOST* to determine the *target ip* and *RPORT* to determine the *target port* to be attacked. To specify the *target Ip* and *port* use the *set* command, as in the following image.



Picture. 6 Display Options
Source : Researcher 2024

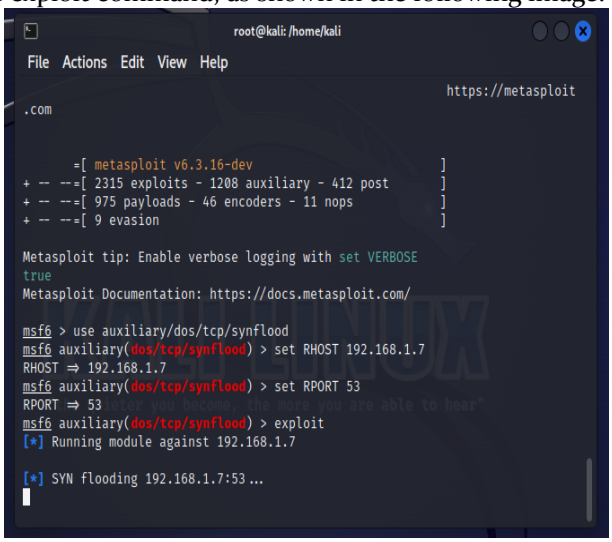
E-ISSN 2962-4274

Fill *RHOST* with target IP / Mikrotic IP and *RPORT* fill with PORT 53



Picture. 7 Target Defining Display
Source : Researcher 2024

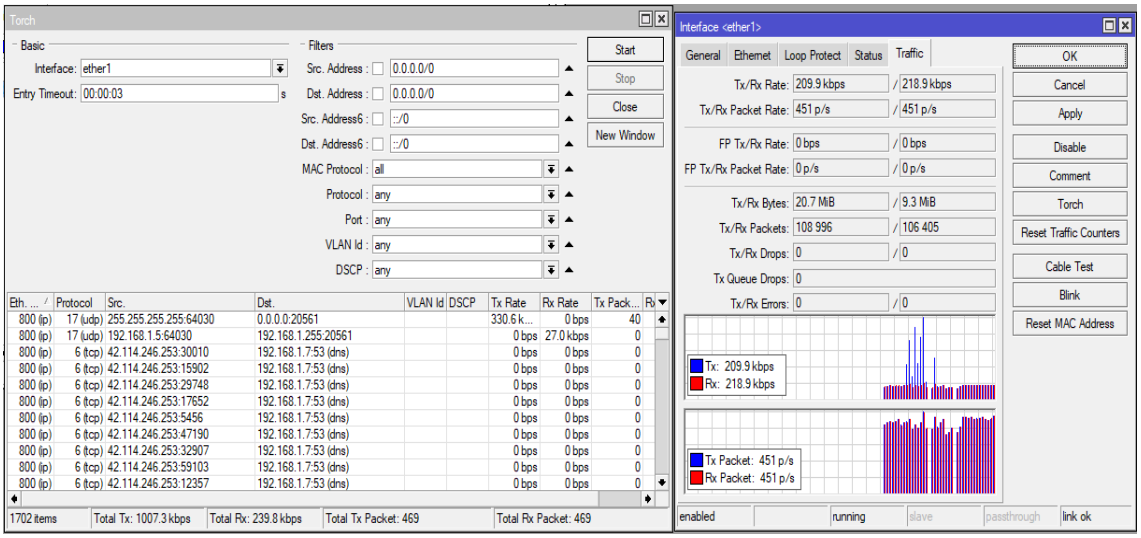
4. Launching an Attack
   Next is to launch an attack after making settings on the available menus. To carry out an attack can use the exploit command, as shown in the following image.



Picture. 8 Launching an Attack Display
Source : Researcher 2024

After carrying out the attack, the next step is to look at the state of *the traffic* as shown in the figure, it can be seen that the traffic that looks abnormal where the *Tx/Rx Rate* value is 209.9 kbps / 218.9 kbps and the *Tx/Rx Packet* value is 451 p/s / 451 p/s. This can be interpreted that the *router device* in terms of *interfaces* is maximally only able to skip data *requested by the user* of 100 Mbps on the *router interface*. Meanwhile, the impact of this DoS attack causes *the interface* to miss 20 Mbps of data. This indicates that *traffic* can no longer pass user access requests to *servers* that go through *the router*.

E-ISSN 2962-4274



Picture. 9 Traffic Appearance during the attack
Source : Researcher 2024

When a DoS attack occurs on the router's network, *the CPU* and *memory* load increases. Based on the results of *the Traffic Monitor System* after the DoS attack, it is known that *the Traffic System Monitor Packet* data *CPU Load* increased to 46% and the *96* MiB Memory increased significantly. This causes *a down* in *Network Traffic* due to *a DoS attack* on the *router*. It can be seen in the following image.

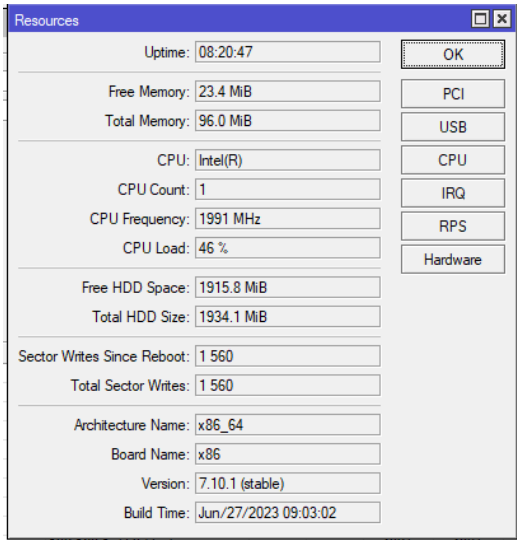


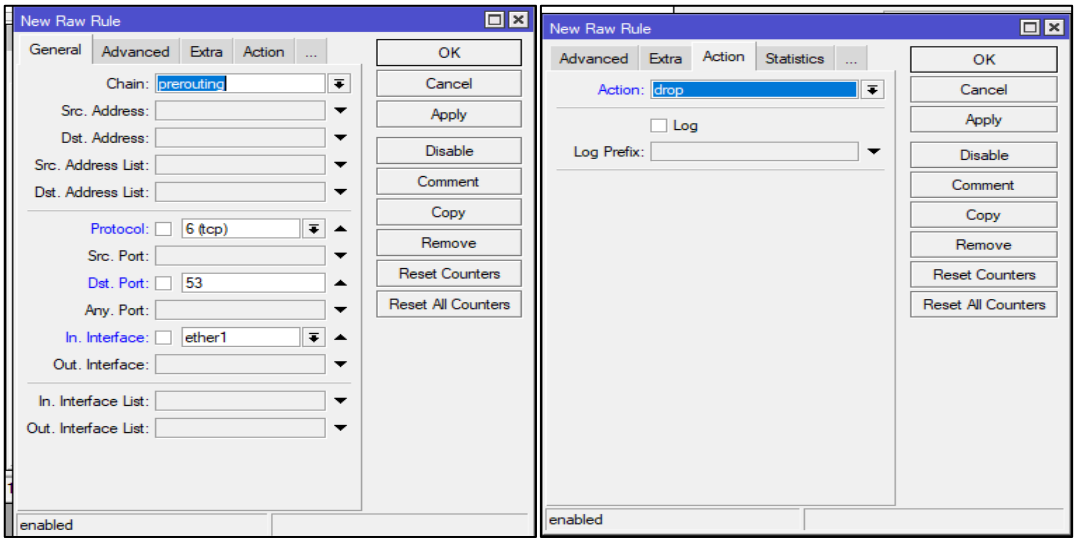
Figure 10 View of Resources during the attack
Source : Researcher 2024

b. Network Security Protection *With MikroTik Router*

From the above problems, the author took action to improve the security of the Router, namely by using the *Firewall Raw* feature on *the MikroTik Router*. *RAW* is a *firewall table* that is similar to a filter table, which handles packet filtering. However, *Raw* has the advantage of not consuming as many CPU resources as the *filter firewall*. *Firewall Raw* is very effective in securing attacks that occur on *MicroTik Routers*. Here are the results of testing *the Syn Flood* attack after using *the Firewall Raw* feature.

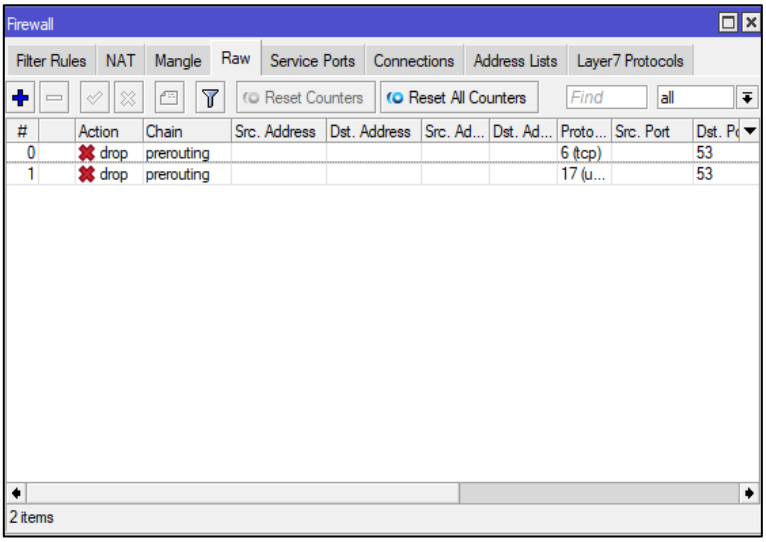
E-ISSN 2962-4274

The steps to run *the Firewall Raw* tool are to go to the *IP > Firewall > Raw menu*, as shown in the following image, for the configuration can be seen in the following image.



Picture. 11 General Settings Display on New Raw Rule
Source : Researcher 2024

Perform the same settings on the other protocols. Once some parameters have been inputted, it will generate a Raw Firewall as seen in the following image.

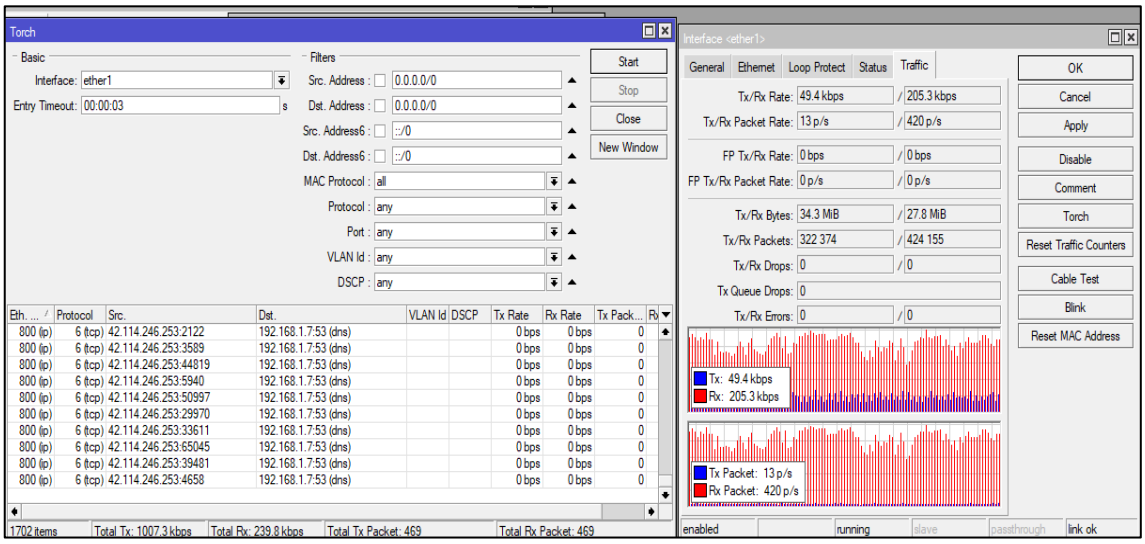


Picture. 12 Raw Firewall Blocked Data Package Display
Source : Researcher 2024

It can be seen in the image above that the author configures 2 types of protocols that are blocked by *Firewall Raw*, namely *the tcp protocol* and *the udp protocol*. This means that when an attacker sends data packets in succession, *Firewall Raw* can prevent the attack by blocking the *IP address* that is suspected of being an attacker so that the attacker's network connection is cut off from the *router*. Furthermore, a test was carried out after using *the Raw Firewall* in the image, it can be seen that in the *Traffic* menu which does look abnormal where the Tx/Rx Rate value is 49 kbps / 205.1 kbps and the

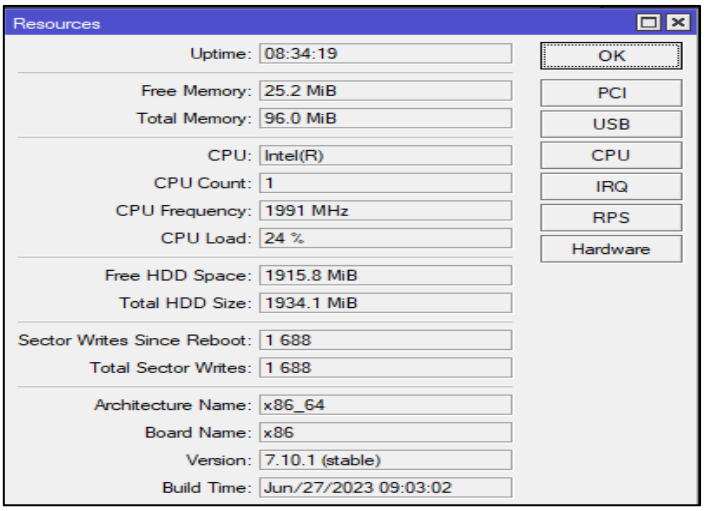
E-ISSN 2962-4274

Tx/Rx Packet value is 13p/s / 420p/s. This is because the attack carried out is still recorded in the graph but the request made is not accepted by *the Router* because the incoming protocol is *TCP* and *UDP protocols* that have been dropped by *Firewall Raw are data that is refused to enter the Router network*.



Picture. 13 Display after using Raw Firewall
Source : Researcher 2024

This proves that *Firewall Raw* is able to block data that is suspected of being sent by an attacker on the *router*'s network. So that *the router* network does not experience down like before using *the Raw Firewall*. The changes that occur to the *router* network when using *the Raw Firewall* can be seen in the following image.



Picture. 14 Displays After Using Raw Firewall
Source : Researcher 2024

In the image, it can be seen that the CPU Load dropped from 46% to 26% after using *the Raw Firewall*. It can be concluded that *Firewall Raw* can prevent DDoS attacks in this case is *a Syn Flood* attack so that the Router does not go *down*

E-ISSN 2962-4274

D. Discussion

Based on the results of the tests that have been carried out, namely conducting DDoS attacks and improving security on Mikrotik Routers using Firewall Raw, the results of the research are presented in the form of a table based on the process that has been carried out. The results of the analysis are summarized in the following table.

Table. 1 Result Analysis

NO.	Analysis	Information
1	The Syn Flood *attack* on *routers* uses *the Metasploit Framework* on *Kali Linux.*	Successfully attacked the router network repeatedly until it brought the network down
2	Successfully breached attack protocols	*TCP and UDP protocols*
3	*Port Destination* target	Port 53
4	The condition of *the CPU* and *Memory* of the network device before it was attacked	*CPU Load 1%* *Memory 96 Mib*
5	CPU and *Memory* conditions of network devices after attack	*CPU Load 46%* *Memory 96 Mib*
6	*Log Activity*	There are quite a few login failures. This activity is suspected to be an abnormal activity that communicates data on the *DNS Protocol* with IP 201.194.230.12 against a Router with a local network IP of 192.168.40.1
7	a. *Attacker's IP Address List* b. *Mikrotik IP Router* c. *IP Network Administrator* d. *IP Router to ISP (Internet Services Provider)* f. *IP Gateway Internet to ISP*	a. 42.114.246.253 b. 192.168.1.7 c. 192.168.1.0 d. 192.168.1.1 f. 192.168.1.1
8	Mikrotik Router Security Enhancements	Using i.
9	CPU and *Memory* conditions of network devices after using *Raw Firewall*	*CPU Load* drops to 46% Memory 96 Mib

4. CONCLUSION

Based on the test results of the use of MikroTik Router as a network security medium from Syn Flood using Firewall Raw, it can be concluded that.

a. The use of Raw Firewall on MikroTik RouterBoard is very effective in securing network systems from attacks, one of which is Syn Flood which carries out attacks by sending SYN request packets to the target machine with the aim of consuming resources from the server which aims to flood the connection limit on the target router.
b. Firewall Raw functions to block IPs that are suspected of sending abnormal data packets on the router's network. This has certainly achieved the author's goal, which is to improve the network security system by using a MikroTik Router which helps in securing and improving protection on the network.

ACKNOWLEDGEMENTS

This research will not be completed without the help of various parties. Therefore, on this occasion, I would like to express my deepest gratitude to those who have provided guidance and direction that have been very useful to me in completing this research. I would also like to express my gratitude to

E-ISSN 2962-4274

my family and friends who have given her support and motivation. Only Allah Almighty can reward him.

REFERENCES

[1] A. Wirawan, C. Feresa, M. Foozy, and A. Azhari, "Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection," vol. 4, no. 1, pp. 1–8, 2020, doi: 10.29099/ijair.v4i1.156.

[2] D. L. Kurdi and B. S. Panca, "Pengujian Performa Komunikasi VoIP Menggunakan Static dan Dynamic Routing Protocol," vol. 2, no. 2009, pp. 111–119, 2020.

[3] M. Ade, C. Rahmani, and S. Prabowo, "Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping dan VLAN," vol. 1, no. 1, pp. 27–37, 2020.

[4] A. Azahro, D. Wulandari, and U. Sari, "NETWORK ADDRESS TRANSLATION PENGHUBUNG IP PUBLIC," no. 1, 2019.

[5] Cloudflare, "What is a DDoS attack?" [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[6] Trivusi, "Serangan DDoS: Pengertian, Dampak, dan Strategi Penanganannya," www.trivusi.web.id. [Online]. Available: https://www.trivusi.web.id/2023/07/ddos-attack.html#:~:text=Dampak dari serangan DDoS dapat,biaya pemulihan infrastruktur yang tinggi.

[7] F. M. and T. T. W. Fuertes, A. Tunala, R. Moncayo, "Software-Based Platform for Education and Training of DDoS Attacks Using Virtual Networks," *Int. Conf. Softw. Secur. Assur. (ICSSA), Altoona, PA, USA*, 2017, doi: 10.1109/ICSSA.2017.19.

[8] P. Pangestu, P. T. Elektro, U. Sultan, and A. Tirtayasa, "ANALISIS OPTIMALISASI KINERJA JARINGAN MAN PADA LAYANAN INTERNET BERBASIS MIKROTIK DI PT. BINA TECHNINDO SOLUTION," vol. 8, no. 1, pp. 8–17, 2021.

[9] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," no. December 2017, 2003.

[10] I. Faisal, "BANDWITH MENGGUNAKAN METODE QUEUE TREE dan PCQ (PER CONNECTION QUEUEING)," vol. 1, no. April 2018, pp. 137–142, 2019.

[11] Fachrid Wadly, Wirda Fitriani, and Muslim, "PERANCANGAN SISTEM RADIUS PADA MIKROTIK ROUTEROS DI PT.PUAN BALEO RAHMADSYAH," vol. 3, pp. 27–35, 2023, [Online]. Available: https://publikasi.hawari.id/index.php/jnastek/article/view/68

[12] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," vol. 2019, 2019.

[13] D. Fitria and M. A. Maulana, "ANALISIS PEMBAGIAN ZONA PROTEKSI PADA JARINGAN DISTRIBUSI 20 kV PENYULANG MERANTI GI BUNGARAN UNTUK MENINGKATKAN PELAYANAN KE KONSUMEN," *J. Ampere*, vol. 5, no. 2, p. 68, 2020, doi: 10.31851/ampere.v5i2.5056.

[14] R. Rizky, A. H. Wibowo, Z. Hakim, and L. Sujai, "Sistem Pakar Diagnosis Kerusakan Jaringan Local Area Network (LAN) Menggunakan Metode Forward Chaining," vol. 7, no. 2, 2019.