Security System Analysis Against Flood Attacks Using TCP, UDP, and ICMP Protocols on Mikrotik Routers

Warid Yunus[1], Mohamad Efendi Lasulika[2]
[1,2] Faculty of Computer Science, Ichsan Gorontalo University, Gorontalo, Indonesia

Article Info

Article history:

Received Feb 24, 2022
Revised Mar 19, 2022
Accepted Apr 30, 2022

Keywords:

Mikrotik
Flooding
DDOS TCP
UDP
ICMP
Firewall

ABSTRACT

Advances in information technology today require all existing computer networks to be able to show that the security system model continues to be considered very important for users who want security both from inside and outside the network. An attack on a network server can occur at any time, as for an attack that can cause a dangerous effect on a router, namely DDOS / flood by flooding the router with very many data packets so that the router can be paralyzed in terms of handling the network system. In this study, descriptive research was applied to obtain data directly by conducting flooding techniques and analyzing and designing flooding prevention techniques with filtering techniques. The application of filtering on the firewall on MikroTik can minimize attacks and prevention directly by dropping flooding packets automatically so that MikroTik performance remains stable.

Corresponding Author:

Mohamad Efendi Lasulika,
fendidsn.ui@gmail.com
Faculty of Computer Science,
Ichsan Gorontalo University

1. INTRODUCTION

The advancement of information technology today requires all computer networks that exist today to be able to show that the security system model continues to be considered very important for users who want security both from inside and outside the network because the internet has very open access in the world and has included invaluable contributions to its users, but it also results in abuse that can harm the users themselves, so that the consequence that must be borne is the guaranteed security of users who are connected directly to the internet network [1].

The use and management of internet-based information technology for Ichsan Gorontalo University are one of the implementations of technology in supporting academic processes and supporting activities in various activities of lecturers and students, but in the internet world there are often negative impacts felt in its use, one of which is the use of weaknesses in network systems, such as hacking of network systems, destruction and even information theft in users who use such internet technology.

Various forms of attacks and even threats directly or indirectly will have an impact on the activities that occur on the internet network, so to protect various forms of possible attacks on the network, a security mode such as a firewall is needed [2].

Firewall itself is a concept of the security system contained in the operating system. The operating system on a computer network is a resource regulatory medium which provides security or protection on the network, as well as being a controller for users to always be able to connect to network sources [3]. While the Firewall is configured to be able to limit unexpected access to the network from inside and outside.

Firewalls have two very important components, namely routers and application gateways. A router is a piece of hardware that has its software in building a system that is a defense for the network, while an application gateway is a special software for observing incoming and incoming packets. The router's ability in terms of running a security system includes packet filtering and proxy services. Packet filtering is a process carried out by tools or software that strictly control the flow of a packet containing information obtained from a network [4].

IP is a transmission mechanism used by TCP / IP protocols, where IP is unreliable, connectionless and datagram delivery service (UDP). Unreliable means that there is no guarantee from the IP protocol for datagrams (Packets located inside the IP layer) that are sent to the destination. The IP protocol strives to get the sent packets to their destination. If in transit, the packet experiences a problem such as the path of the path being cut off, there will be a buildup on the router or target host down, then the TCP protocol can only inform the sender of the packet through the ICMP protocol that there has been a problem in terms of sending the IP packet [5].

These packages if they cannot be secured can be used by anyone or irresponsible people in doing things that endanger the network system, such as by manipulating packets or sending large amounts of packets on certain protocols that can weaken the network system or go down. With the initial analysis of the network protocols on the firewall, namely the TCP, UDP, and ICMP protocols, it is hoped that it can measure the effectiveness of firewall performance in terms of filtering packets that come in and out to minimize network security problems on the Mikrotik router.

In this study, the authors used a router device and a Mirotic operating system that has been integrated. Mikrotik router is one of the operating systems that can be used as a reliable network router because there are various complete features for computer networks besides that Mikrotik also has a function as a firewall [6]. The purpose of this study is to analyze the existing protocols on the network, namely TCP, UDP, and ICMP, then implement a filtering packet-based security system as a firewall on the MikroTik, then test performance analysis to measure the capabilities of the firewall and to determine the performance of incoming traffic on the router.

2. RESEARCH METHOD

2.1. Computer Network

A computer network is a group of computers and other network devices connected in one unit that works together in achieving a common goal, namely the exchange of information and data through a connecting medium using cables or wireless so that computer network users can exchange data and information together and can even use hardware/software connected to the network together. Each computer or device connected to the network is called a node. A computer network can have two, tens, thousands, or even millions of nodes [7].

To achieve the same goal, each part of the computer network makes requests and service delivery (service). The party who requests the service is called the client (client) and the one who provides the service is called the server (server). This architecture is called a client-server system and is used in all computer network applications. Meanwhile, computer networks can be classified based on their scalability, namely PAN (Personal Area Network), CAN (Campus Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), and finally WAN (Wide Area Network) [8].

2.2. TCP/ IP

TCP/IP was developed referring to the Open System Interconnection (OSI) model, where, the layers contained in TCP are not exactly the same as the layers contained in the OSI model. There are four layers in TCP / IP, namely: network interface, network, transport and application. The first three layers of TCP/IP provide physical standards, network interfaces, internetworking, and transport functions, which refer to the first four layers of the OSI model. The top three layers of the OSI model are represented in the TCP/IP model as one layer, namely the application layer [9].

2.3. OSI Layer Protocol

Open System Interconnection is an open system that is a set of protocols that can be interconnected with two different systems that come from different architectures but can also be interpreted as a group of protocols that create two different systems to communicate regardless of the design of the system below. Created by the International Standards Organization (ISO). OSI is only a protocol model, not a usable protocol [10].

The purpose of OSI is to facilitate communication to be established from different systems even without the need for significant changes to each hardware and software at the main level.

2.4. TCP Protocol

It is a standard in the form of data communication used by communities on the internet network in the process of exchanging data packets from one computer to another on the internet network. This protocol cannot stand alone, because indeed this protocol is a collection of protocols. This protocol is also the most widely used type of protocol today. And the data is implemented into a form of software on the operating system[11]. Another term given to this software is the TCP/IP stack. In TCP / IP, there are several sub-protocols that deal with communication problems between computers. TCP/IP implements a multi-layered architecture consisting of four layers, including.

1. Application layer protocol
2. Inter-host layer protocol
3. Internetwork layer protocol
4. Network interface layer protocol

2.5. UDP Protocol

User Datagram Protocol (UDP) is a TCP/IP transport layer protocol that supports unreliable communication, connectionless between each host in the network that uses the TCP IP protocol [12].

1. User Datagram Protocol Provides checksum calculations with a size of 16 bits on the entire UDP message
2. User Datagram Protocol provides a mechanism for sending messages to one of the application layers protocols or certain processes on hosts on the network that uses TCP IP
3. Unreliable, UDP messages will be sent as a datagram without any sequence of numbers or notification messages. The protocol application layer running on UDP must recover messages lost during the transmission process
4. Connectionless, UDP messages are sent without having to be carried out the process of negotiating a connection between hosts who will exchange information

2.6. ICMP Protocol

ICMP is a core protocol of the family. ICMP is different in purpose to TCP and UDP in that icmp is not used directly by the user's network application. one exception is a ping application that sends an ICMP Echo Request message (and receives an Echo Reply) to determine whether the destination computer is reachable and how long the packet sent is replied to by the destination computer. internet protocol. ICMP is primarily used by networked computer operating systems to send error messages stating, for example, that the destination computer is unreachable [13].

2.7. Network Security

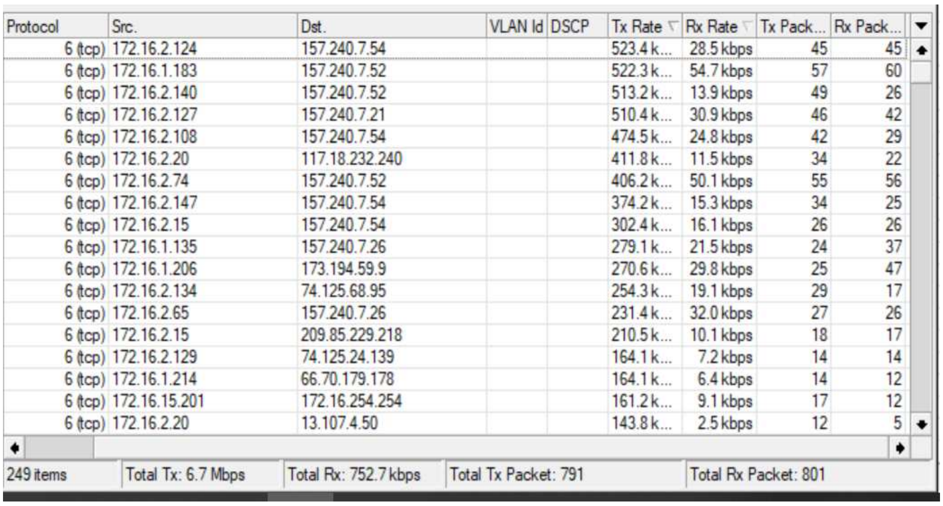
Computer network security is the process of preventing and identifying uses that do not have a valid permit from a computer network. precautions are taken to help stop unauthorized users from accessing any part of the computer network. The purpose of computer network security is to be able to anticipate the occurrence of risks to computer networks in the form of threats either physically or logically that directly or indirectly interfere with the activities that are running on the computer network system.

There are several aspects of security in a computer network, namely Confidentiality, Integrity, Available, Non-Repudiation, Authentication, Access Control, Accountability. As for the types of attacks or security threats on the network, there are several of them, namely Denial of Service (DOS), Distributed Denial of Service (DDOS), SYN Flooding, UDP Fooding, Flooding ICMP, IP Spoofing, Sniffing, Port Scanning, Hijacking, and finally Trojan [13].

3. RESULTS AND DISCUSSION

3.1. Data Collection Results

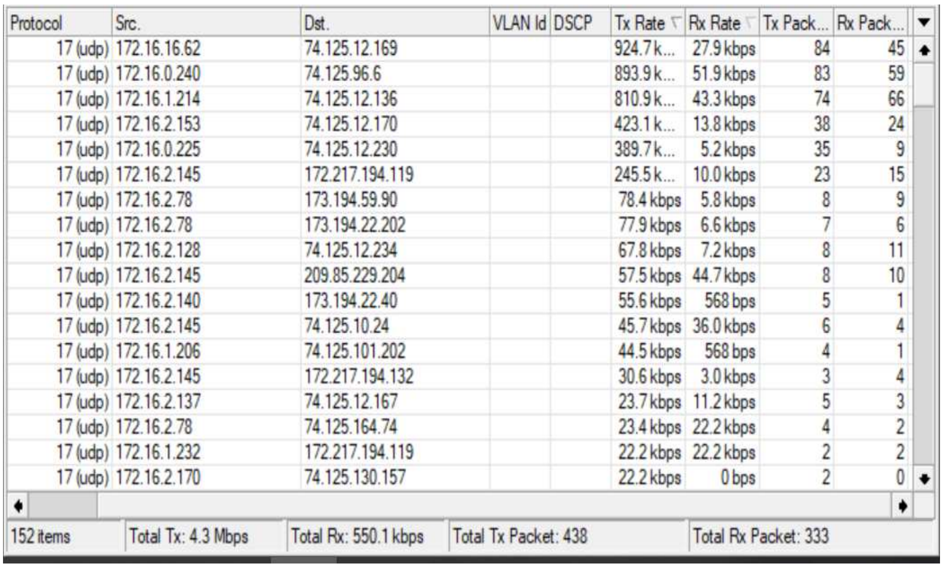
The following are the results of data traffic collection on the TCP, UDP and ICMP protocols through direct observation on the MikroTik router of Ichsan Gorontalo University which then the data is captured and can be seen in the following picture.



Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
6 (tcp)	172.16.2.124	157.240.7.54			523.4 k...	28.5 kbps	45	45
6 (tcp)	172.16.1.183	157.240.7.52			522.3 k...	54.7 kbps	57	60
6 (tcp)	172.16.2.140	157.240.7.52			513.2 k...	13.9 kbps	49	26
6 (tcp)	172.16.2.127	157.240.7.21			510.4 k...	30.9 kbps	46	42
6 (tcp)	172.16.2.108	157.240.7.54			474.5 k...	24.8 kbps	42	29
6 (tcp)	172.16.2.20	117.18.232.240			411.8 k...	11.5 kbps	34	22
6 (tcp)	172.16.2.74	157.240.7.52			406.2 k...	50.1 kbps	55	56
6 (tcp)	172.16.2.147	157.240.7.54			374.2 k...	15.3 kbps	34	25
6 (tcp)	172.16.2.15	157.240.7.54			302.4 k...	16.1 kbps	26	26
6 (tcp)	172.16.1.135	157.240.7.26			279.1 k...	21.5 kbps	24	37
6 (tcp)	172.16.1.206	173.194.59.9			270.6 k...	29.8 kbps	25	47
6 (tcp)	172.16.2.134	74.125.68.95			254.3 k...	19.1 kbps	29	17
6 (tcp)	172.16.2.65	157.240.7.26			231.4 k...	32.0 kbps	27	26
6 (tcp)	172.16.2.15	209.85.229.218			210.5 k...	10.1 kbps	18	17
6 (tcp)	172.16.2.129	74.125.24.139			164.1 k...	7.2 kbps	14	14
6 (tcp)	172.16.1.214	66.70.179.178			164.1 k...	6.4 kbps	14	12
6 (tcp)	172.16.15.201	172.16.254.254			161.2 k...	9.1 kbps	17	12
6 (tcp)	172.16.2.20	13.107.4.50			143.8 k...	2.5 kbps	12	5

249 items | Total Tx: 6.7 Mbps | Total Rx: 752.7 kbps | Total Tx Packet: 791 | Total Rx Packet: 801

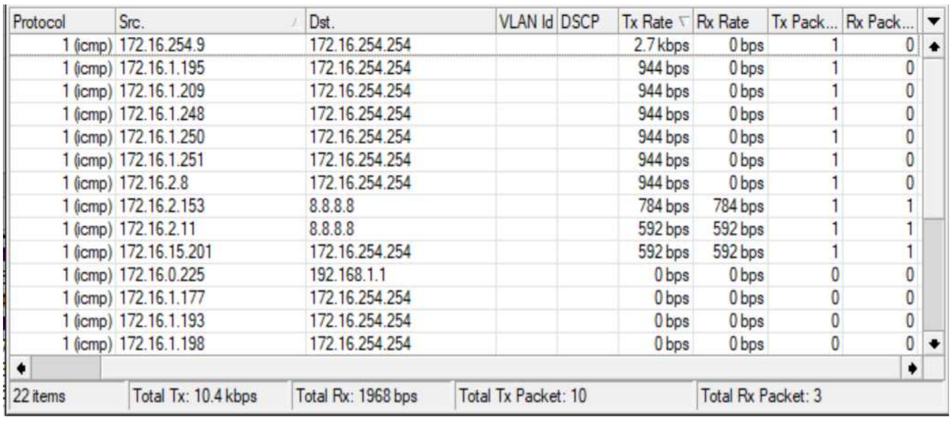
Figure 1. Trafic Data on TCP Protocol



Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
17 (udp)	172.16.16.62	74.125.12.169			924.7 k...	27.9 kbps	84	45
17 (udp)	172.16.0.240	74.125.96.6			893.9 k...	51.9 kbps	83	59
17 (udp)	172.16.1.214	74.125.12.136			810.9 k...	43.3 kbps	74	66
17 (udp)	172.16.2.153	74.125.12.170			423.1 k...	13.8 kbps	38	24
17 (udp)	172.16.0.225	74.125.12.230			389.7 k...	5.2 kbps	35	9
17 (udp)	172.16.2.145	172.217.194.119			245.5 k...	10.0 kbps	23	15
17 (udp)	172.16.2.78	173.194.59.90			78.4 kbps	5.8 kbps	8	9
17 (udp)	172.16.2.78	173.194.22.202			77.9 kbps	6.6 kbps	7	6
17 (udp)	172.16.2.128	74.125.12.234			67.8 kbps	7.2 kbps	8	11
17 (udp)	172.16.2.145	209.85.229.204			57.5 kbps	44.7 kbps	8	10
17 (udp)	172.16.2.140	173.194.22.40			55.6 kbps	568 bps	5	1
17 (udp)	172.16.2.145	74.125.10.24			45.7 kbps	36.0 kbps	6	4
17 (udp)	172.16.1.206	74.125.101.202			44.5 kbps	568 bps	4	1
17 (udp)	172.16.2.145	172.217.194.132			30.6 kbps	3.0 kbps	3	4
17 (udp)	172.16.2.137	74.125.12.167			23.7 kbps	11.2 kbps	5	3
17 (udp)	172.16.2.78	74.125.164.74			23.4 kbps	22.2 kbps	4	2
17 (udp)	172.16.1.232	172.217.194.119			22.2 kbps	22.2 kbps	2	2
17 (udp)	172.16.2.170	74.125.130.157			22.2 kbps	0 bps	2	0

152 items | Total Tx: 4.3 Mbps | Total Rx: 550.1 kbps | Total Tx Packet: 438 | Total Rx Packet: 333

Figure 2 Trafic Data on UDP Protocol



Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
1 (icmp)	172.16.254.9	172.16.254.254			2.7 kbps	0 bps	1	0
1 (icmp)	172.16.1.195	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.1.209	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.1.248	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.1.250	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.1.251	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.2.8	172.16.254.254			944 bps	0 bps	1	0
1 (icmp)	172.16.2.153	8.8.8.8			784 bps	784 bps	1	1
1 (icmp)	172.16.2.11	8.8.8.8			592 bps	592 bps	1	1
1 (icmp)	172.16.15.201	172.16.254.254			592 bps	592 bps	1	1
1 (icmp)	172.16.0.225	192.168.1.1			0 bps	0 bps	0	0
1 (icmp)	172.16.1.177	172.16.254.254			0 bps	0 bps	0	0
1 (icmp)	172.16.1.193	172.16.254.254			0 bps	0 bps	0	0
1 (icmp)	172.16.1.198	172.16.254.254			0 bps	0 bps	0	0

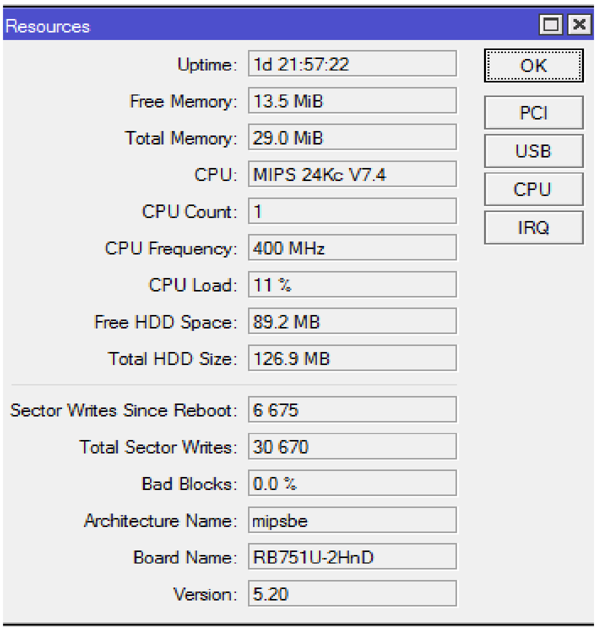
22 items | Total Tx: 10.4 kbps | Total Rx: 1968 bps | Total Tx Packet: 10 | Total Rx Packet: 3

Figure 3 Trafic Data on ICMP Protocol

From the image information above, it is concluded that data traffic on the TCP protocol runs normally, it is based on the amount of Tx Rate and Rx rate in accordance with the limitations applied at the Ichsan Gorontalo university Pustikom, and traffic using the ICMP protocol is also still normal from client ping requests. Meanwhile, traffic using the UDP protocol, the author feels that there is no reason because the normal limit of UDP traffic is below 1 Mbps. So it is necessary to carry out further analysis and identification of traffic that exceeds the normal limit.

3.2. Model Discussion

In the Flooding Experiment on TCP, UDP, and ICMP protocols in the MikroTik router at Ichsan Gorontalo University, monitoring the status of resources or the use of MikroTik resources was obtained in the form of CPU Load of 11% and a total memory of 29Mb on router activities in a busy state by serving 50-70 active users.



Uptime: 1d 21:57:22
Free Memory: 13.5 MiB
Total Memory: 29.0 MiB
CPU: MIPS 24Kc V7.4
CPU Count: 1
CPU Frequency: 400 MHz
CPU Load: 11 %
Free HDD Space: 89.2 MB
Total HDD Size: 126.9 MB
Sector Writes Since Reboot: 6 675
Total Sector Writes: 30 670
Bad Blocks: 0.0 %
Architecture Name: mipsbe
Board Name: RB751U-2HnD
Version: 5.20

Figure 4. Status of Mikrotik Resources Under Normal Circumstances

3.3. Model Test Results

3.3.1. Flooding Protocol Mikrotik Without Filtering

The results of experiments and testing of the flooding protocol mikrotik without filtering on TCP, UDP, and ICMP are shown in Table 1, Table 2, and Table 3, respectively.

Table 1. Unfiltered TCP Flood Packet Testing Data

IP Address	Number of TCP Packets	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	-+30mbps	-+25mbps	-+30mbps	40 %	Yes
172.16.40.90	-+50mbps	-+50mbps	-+50mbps	60 %	Yes
172.16.33.20	-+75mbps	-+75mbps	-+75mbps	60 %	Yes

Testing the firewall system against flooding was carried out using UDP unicorn tools. Unicorn UDP tools were chosen because they are proven to be able to flood or be able to send as many UDP and TCP packets as possible to the intended router. The first test was carried out without enabling the filtering function in the firewall with the following parameters used:

Target = Mikrotik IP address 172.16.254.254
Protocol = TCP & UDP
Port = DNS (53)
Packet Size = Random
Delay = 10 ms
Threadd = 1
Socket = 1

From the test results of flood attacks on Mikrotik, UDP traffic has increased beyond the normal limit based on the amount of data sent from the unicorn tool, for the results of the Flood Packet UDP Without Filtering test data can be seen in the Table 2 below.

Table 2. Unfiltered UDP Flood Packet Test Data

IP Address	Number of UDP Packet Attacks	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	65 Kb	0 mbps	-+30mbps	60 %	Yes
172.16.40.90	50 Kb	0 mbps	-+20mbps	45 %	Yes
172.16.33.20	30 Kb	0 mbps	-+20mbps	33 %	Yes

In the Table 3 below, Testing the firewall system against ICMP flooding was carried out with the ping of death technique, namely using the command prompt tool with the command 'ping –l 65500 172.16.254.254 –t'. The description of the command is as follows:

- -l 65500 : the amount of data to be pinged to the router IP with a range of 0-65500
- 172.16.254.254 : IP router MikroTik
- -t : continuous repetition until dismissed

From the test results of flood attacks on the ICMP protocol, it can be seen that ICMP packet traffic has increased from the normal limit to 520kbps.

Table 3. Unfiltered Internet Control Message Protocol (ICMP) Flood Packet Testing Data

IP Address	Number of Icmp Packet Attacks	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	500	4 kbps	4 kbps	50%	Yes
172.16.40.90	1000	8 kbps	8 kbps	50%	Yes
172.16.33.20	50000	818 kbps	576 kbps	50%	Yes

3.3.1. Flooding Protocol Mikrotik with Filtering

While the results of experiments and testing of the flooding protocol mikrotik with filtering on TCP, UDP, and ICMP are shown in Table 4, Table 5, and Table 6, respectively.

Table 4. TCP Flood Packet Testing Data with Filtering

IP Address	Number of TCP Packets	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	-+30mbps	-+25mbps	-+30mbps	40 %	Yes
172.16.40.90	-+50mbps	-+50mbps	-+50mbps	60 %	Yes
172.16.33.20	-+75mbps	-+75mbps	-+75mbps	60 %	Yes

Furthermore, the test used filtering techniques by conducting the same attack experiment and the traffic results received by Mikrotik looked normal, even the UDP flood did not enter the router.

Table 5. Flood Packet UDP Testing Data with Filtering

IP Address	Number of UDP Packet Attacks	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	65 Kb	0 mbps	-+30mbps	60 %	No
172.16.40.90	50 Kb	0 mbps	-+20mbps	45 %	No
172.16.33.20	30 Kb	0 mbps	-+20mbps	33 %	No

In addition, the test used filtering techniques while still conducting an attack experiment that flooded the same ICMP and the traffic results received by Mikrotik looked normal with traffic of 13kbps.

Table 6. ICMP Flood Packet Testing Data with Filtering

IP Address	Number of Icmp Packet Attacks	Status Traffic		Status Resource Mikrotik	Connect tracking
		Tx Rate	**Rx Rate**	**CPu Load**	
172.16.0.24	500	4 kbps	4 kbps	50%	No
172.16.40.90	1000	8 kbps	8 kbps	50%	No
172.16.33.20	50000	818 kbps	576 kbps	50%	No

4. CONCLUSION

Based on the results of research conducted on the MikroTik router Pustikom Ichsan Gorontalo University and the discussion that has been described earlier, it can be concluded that in general, a filtering-based firewall system against flooding attacks on the TCP, UDP and ICMP protocols that are applied has succeeded in preventing flood attacks.

From the results of the performance analysis obtained in the application of the filtering protocol applied in the MikroTik router firewall, for flooding attacks on the TCP Protocol, it is still difficult to recognize incoming data traffic, because the TCP protocol is used in conjunction with browsing access and downloads by the client. As for the UDP and ICMP traffic protocols, it is easier to recognize so that the filtering rule applied to the firewall automatically drops the flood packet. several suggestions need to be considered to achieve the expected goals, namely this Filtering System can be developed by filtering protocols that can cause flood attacks other than TCP, UDP, and ICMP and to Improve Firewall Performance Based on This Filtering can be used or combined with other flood attacks monitoring systems such as IDS and IPS.

REFERENCES

[1] B. Stott, O. Alsac, and A. J. Monticelli, “Security analysis and optimization,” *Proceedings of the IEEE*, vol. 75, no. 12, pp. 1623–1644, 1987, doi: 10.1109/proc.1987.13931.

[2] N. R. Potlapally, S. Ravi, A. Raghunathan, R. B. Lee, and N. K. Jha, “Configuration and Extension of Embedded Processors to Optimize IPSec Protocol Execution,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 15, no. 5, pp. 605–609, May 2007, doi: 10.1109/tvlsi.2007.896912.

[3] S. Agustini and A. Mudzakir, “Network Security with Firewall using MikroTik RB941,” *e-NARODROID*, vol. 4, no. 2, pp. 13–24, Sep. 2018, doi: 10.31090/narodroid.v4i2.730.

[4] D. Aprilianto, T. Fadila, and M. A. Muslim, “Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik,” *Techno.com*, vol. 16, no. 2, pp. 114–119, Jan. 2017, doi: 10.33633/tc.v16i2.1291.

[5] S. Awang Nor, R. Alubady, and W. Abduladeem Kamil, “Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network,” *Procedia Computer Science*, vol. 111, pp. 2–7, 2017, doi: 10.1016/j.procs.2017.06.002.

[6] R. R and Y. Muin, “MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method,” *International Journal of Computer Applications*, vol. 183, no. 47, pp. 33–37, Jan. 2022, doi: 10.5120/ijca2022921878.

[7] Wecker, “Computer Network Architectures,” *Computer*, vol. 12, no. 9, pp. 58–72, Sep. 1979, doi: 10.1109/mc.1979.1658895.

[8] D. Comer, *Computer Networks And Internets*. Boston, Massachusetts: Pearson, 2015.

[9] D. Comer, *Internetworking with TCP/IP*. Upper Saddle River: Pearson Education Inc, 2014.

[10] C. I'anson and A. Pell, *Understanding OSI applications*. Englewood Cliffs, N.J.: Ptr Prentice Hall, 1993.

[11] M. G. Naugle, *Network protocol handbook*. New York: Mcgraw-Hill, 1994.

[12] W. Tomasi, *Advanced electronic communications systems*. Upper Saddle River, N.J.: Prentice Hall, 2001.

[13] B. A. Forouzan and Sophia Chung Fegan, *TCP/IP protocol suite*. Boston, Mass.: Mcgraw-Hill, C, 2007.