Implementation of MikroTik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks of Al-Mahrusiyah Vocational School Lirboyo

Asyiq Maulana[1], Nugroho Suharto [2], Aad Hariyadi [3]

[1]Digital Telecommunication Network Study Program, [2,3]Telecommunication Engineering Study Program
Electrical Engineering, Malang State Polytechnic, Indonesia

[1]asyiq.emciay@gmail.com, [2]nugroho.suharto@polinema.ac.id, [3]aad.hariyadi@polinema.ac.id

***Abstract*— Internet access is so easy that every level of society can access information from the website. If internet access is used positively, it will produce positive things for its users as well. Such as the facilities provided by the management of SMK Al-Mahrusiyah Lirboyo. Students, especially in the Computer and Network Engineering (TKJ) department, get facilities such as PCs in the lab or laptops along with internet access during productive learning hours. In its application in schools, students who are given laptop facilities and internet access do not always use it for learning. Questionnaire data showed that there were other things that were accessed, including 37.7% of respondents finding and trying hacking tutorials, 35.8% playing social media, and 34% streaming movies. For this reason, a firewall is needed that restricts students' access to it. The firewall will be formulated with a script on the MikroTik router through the WinBox. The results of firewall tests using a combination of filters and Raw successfully blocked access to social media websites, streaming movies, and anime. The client cannot access and the display in the client browser displays continuous loading. Testing firewalls to ward off DoS attacks was also successful. When tested, LOIC did not send a single request packet and when the CPU resource was checked, the resource was only 1%. The use of firewalls with MikroTik routers is effective in limiting students' access to other things outside of learning. With this, it is hoped that students can better utilize facilities for learning.**

Keywords*— *Firewall, Mikrotik, LOIC, DoS, Access Restriction

I. INTRODUCTION

Along with the development of today's technology, internet users are increasing, from top to bottom. Internet access is so easy that every level of society can access information from any website just through a smartphone. The information presented on the internet should be divided into positive and negative information. If internet access is used positively and does not violate the rules, it will also produce positive things for its users [1]. For example, if internet access is provided to students, it would be better for students to use it as a means for learning.

Such as the facilities provided by the management of SMK Al-Mahrusiyah Lirboyo. SMK Al-Mahrusiyah Lirboyo is a private school under the auspices of the Lirboyo Al-Mahrusiyah Foundation. Students who attend school are students who live in the SMK environment. Students who attend school, especially in the Department of Computer and Network Engineering (TKJ) and the Department of Multimedia, get facilities in the form of a PC in the lab or laptop along with internet access during the productive study hours of the department. During other hours, such as other subjects or during non-school hours, students are not provided with laptop facilities and internet access. This is intended so that students are more focused on learning and reciting.

In its application in schools, students who are given laptop facilities and internet access do not always use them to study. There is always something else unlocked when using the internet. For example, accessing social media to contact family. In fact, in Pondok, it is only allowed to contact the family through the lodge administrator. This is intended to prevent misunderstandings between students and their guardians and also to ensure that any information submitted is valid. Students who are access to other things when given internet access become distracted and interfere with the learning process.

Students who are given internet access, especially TKJ majors, sometimes also look for something related to hacking because of their high curiosity and maybe because of stereotypes related to hacking. Students generally look for tutorials for hacking WiFi or network attacks. The easiest example is students using internet access to search for router DoS tools with excess packets so that routers are overwhelmed. This makes the router rise dramatically and makes the router heat up quickly. As a result, when the CPU load increases

dramatically, the router cannot properly serve network packets [2][3].

Research conducted by Aznar Abdillah describes the application of a firewall to limit students' Internet access to several websites to create a healthy internet in an educational environment [1]. Meanwhile, research conducted by Budi Jaya explains the use of firewall and Raw filters to overcome DoS attacks on the network. Budi Jaya configures the firewall using the MikroTik script.

From the description above, a study was made that will design a separate network with the implementation of a firewall on the MikroTik Routerboard. The firewall serves to restrict students' Internet access so that they do not wander outside of their learning needs and to counter DoS attacks from intranet networks. The firewall will use a combination of raw and filter rule. The new one is usage of domain content as a reference of sites blocking. All firewall configuration is done with a script in the WinBox Terminal. MikroTik script is easily customized with actual circumstance so it will fit for the school.

II. METHOD

A. Stages of Research

The stages of research carried out as an initial stage in conducting research, are shown below. Everything related to research must be planned in advance, from searching for references to making reports. This stage of research is shown in Fig. 1 below.

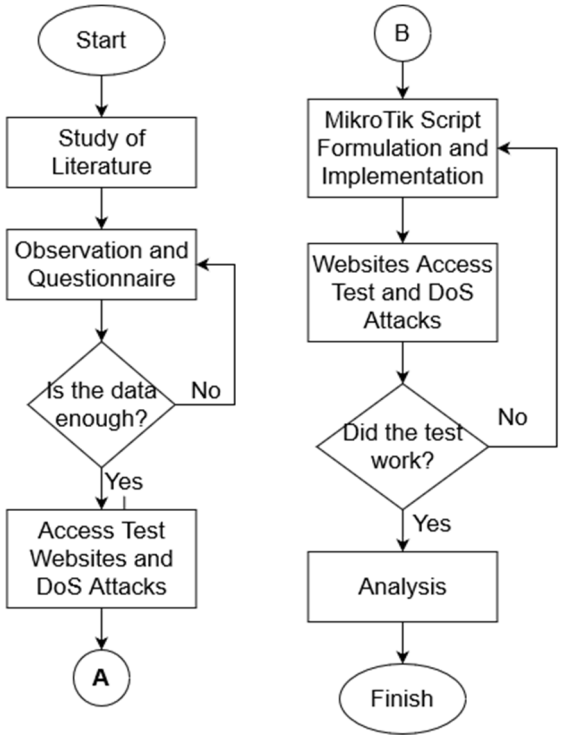

Figure 1. Stages of Research

1) *The first stage:* the identification of problems that arise on the internet network of Al-Mahrusiyah Vocational School

2) The second stage: a study of literature from journals and website articles on issues related to problems, such as MikroTik, routers, and firewalls.

3) *The third stage:* determining the research objectives, namely solving problems that exist on the internet network of Al-Mahrusiyah Vocational School

4) *The fourth stage:* observation. Observations were carried out directly on teachers and in the Al-Mahrusiyah Vocational School as well as on several alumni to get validation from problems. If the observation data is lacking, the observation is carried out more deeply. If the observation data is sufficient, then proceed to the next process.

5) *The fifth stage:* the collection of supporting data from the results of observations

6) *The sixth stage:* system design after knowing the problem and valid data from observations

7) *The seventh stage:* system testing in the lab. Al-Mahrusiyah SMK computer. If the test has not been successful, then return to the system design stage with improvements. If successful, then proceed to the next process.

8) The eighth stage: the analysis of the system test results

9) *The ninth stage:* the formulation of conclusions on the report

To support blocking websites through firewalls, a literature was conducted to obtain domains for social media and streaming sites. This domain is configured in the Raw filter in the ***"content="*** script to get the public IP of each connection towards that domain. Domain content is obtained from BILHANET [4][5][6] which provides many useful articles about networking. The list of some content domains is written in the Table 1.

TABLE 1
DOMAIN CONTENTS

Site	Domain Contents
Facebook	facebook.com, .facebook.net, .fbcdn.net, .fbsbx.com, fb.com, fb.gg, fbwat.ch, messenger.com, m.me
Instagram	.instagram.com, .cdninstagram.com
Twitter	twitter.com, .twitter.com, .twimg.com, t.co
LK21	116.203.17.158
idlix	37.49.229.132

B. System Planning

In this study, there is a research network topology that is used as an illustration of hardware connection and there is a firewall system block diagram for restricting access to websites and a RAW firewall block diagram for dealing with DoS attacks [7]. The network topology is shown in Fig. 2.

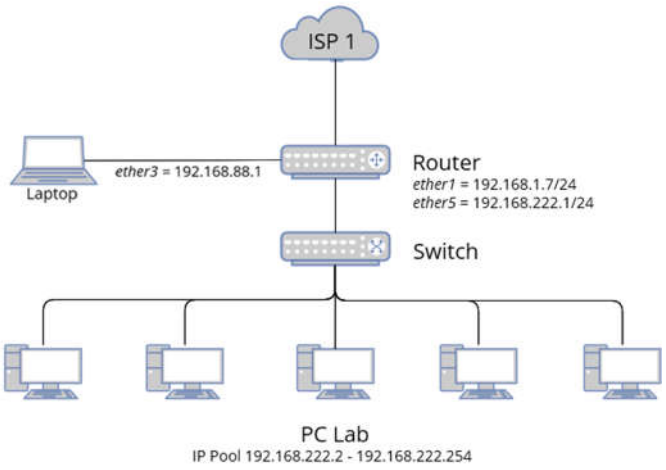

Figure 2. System Planning

ISP is an internet service provider installed in SMK Al-Mahrusiyah. In this study, only 1 ISP is connected to a MikroTik router on ether1. ether3 MikroTik is connected to a laptop to configure with scripts from WinBox. Then the MikroTik ether5 is connected to the switch to extend the reach to the client. From the switch is connected directly to each PC in the lab. Computer.

The firewall diagram block for restricting access to certain websites is shown in Fig. 3.

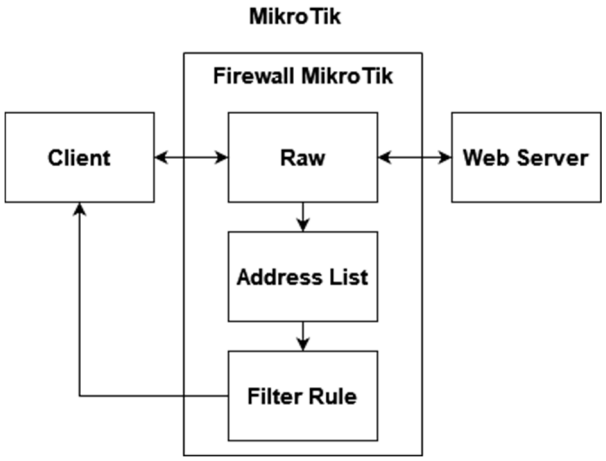

Figure 3. Diagram Block of Blocking Website System

The client is an internet user which in this case is a PC in the lab. computer. In this test, the client accesses the desired website when given internet access. When the client accesses the website, the Raw filter will read the domain and get the website's public IP [8]. Raw works according to the established rules. The rules are obtained from observations regarding what website access is not allowed to students when given internet access. If the website being accessed is not in the Raw rule, then the client can access the website. However, if the website being accessed does not match the existing rules in Raw, Raw will send the public IP of the website being accessed to the Address List [9]. In the Address List, all the public IPs of the domains set in the Raw rule are listed. Then, filter rule work as a blocker for all IPs listed in address list [10][11].

And then here is the block diagram of a RAW firewall to prevent DoS attacks is shown in Fig. 4.

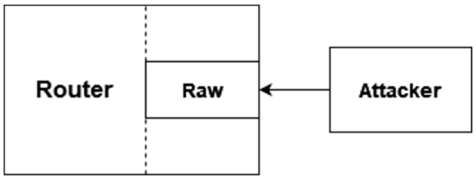

Figure 4. Diagram Block of DoS Prevention

Attacker (attacker) comes from one of the PCs in the lab. computer. The attacker performs a DoS attack on the router with the LOIC software running on the Windows operating system [12]. The attacker sends as many TCP and UDP packets to the router as possible to maximize the router's CPU resources [13]. The RAW firewall serves to ward off redundant TCP and UDP packets. The goal is for CPU resources to work normally.

C. Procedure of Testing

The procedure of this research is to ensure all PCs in the lab. computer is connected via a room switch. Switch port 1 is connected to the MikroTik router ether5 that has been configured with the MikroTik script. ether1 router is connected to internet source from ISP. After that, testing the website access from the PC lab. computer done. Next, testing of DoS attacks is done by installing LOIC software on one PC. From the LOIC software, a DoS attack is carried out by sending as many TCP and UDP packets as possible to the router. CPU resource changes in MikroTik are monitored from WinBox on a laptop connected to an ether3 router

III. RESULTS AND DISCUSSION

A. Observation Result

Observation results were obtained from interviews with several alumni of the Computer Network Engineering (TKJ) department of SMK Al-Mahrusiyah on July 31, 2022. Then the interview continued with Mr. Farid as the Principal, Mrs. Ninik as Deputy Head of Curriculum, Mr. Ahmad Yanwar Syarif as Productive Teacher on 1 August 2022.

When interviews were conducted with alumni of the TKJ department named Dwiky and Abdul Aziz, the researchers asked if they had ever accessed anything other than learning when they were given internet access. They confirmed that they frequently access other things when given internet access. They access social media to connect with friends or family and access movie streaming websites as entertainment when studying. They have also tried hacking tutorials or attacks on computer networks from articles during productive hours [14].

When the researcher asked for permission to observe the principal, he allowed it but limited data collection to only be done in the first lab. computer without students being there. This caused at that time students who had productive hours

worked on the national assessment simulation so they could not be disturbed. Next, the researcher was directed to Mrs. Ninik and the researcher conducted a fairly short interview. When asked about school rules when students were given facilities, he said that the rules at school did not allow students who had laptop and internet facilities to access other things outside of learning field, especially entertainment. This is not without reason because the purpose of providing facilities is to support learning to be more productive.

Then, the researcher continued the interview with Mr. Ahmad Yanwar. The researcher asked about what students did when they were given internet access facilities. He said that he frequently caught students accessing other things outside of learning. Many teachers have reminded verbally. However, when they are separated from supervision, students immediately use their inattention to access other things. Mr. Ahmad Yanwar's attempt to block the website was not effective enough beause he used old solution, so another solution was needed to block the website. Mr. Ahmad Yanwar has also seen that the CPU resource of the main router has increased by more than 80% for some time whereas normally the main router only uses 0-2% CPU. When it checked on MikroTik, there was a barrage of connections from one of the clients. He suspected that it came from a student dabbling in a DoS attack. He only blocked the IP and has not implemented a firewall to deal with DoS attacks [15].

From the description of the observations in the paragraph above, it can be concluded that the problems of students who access things outside of learning are confirmed to be valid because the alumni of the TKJ major acknowledge this.

B. Questionnaire Result

This study produces data regarding the answers of respondents from questions about the habits of TKJ students or alumni when given internet access facilities during productive hours. Questionnaires were distributed limited to 12th grade TKJ students and some alumni through the google form. Questionnaire data get a total of 53 respondents.

TABLE 2
QUESTIONNAIRE QUESTIONS

Number	Question
1	What things have you accessed when given internet access facilities during productive hours?
2	Why do you access social media?
3	If you access an article other than learning, what articles do you read?
4	What movie/series/anime streaming websites do you often access?
5	Do you frequently play games during productive hours?
6	If you have ever searched for an article / tutorial about hacking, what tutorials have you read/tried?
7	Why are you looking for articles/tutorials about hacking?

Questionnaire questions refer to the results of observations and matters relating to research. The result of the questionnaire shown in Table 3.

TABLE 3
QUESTIONNAIRE RESULT

Question	Respondents	Result
1	53 (100%)	45.3% browsing for educational purpose 37.7% looking for hacking tutorials
2	34 (64%)	35.8% watching educational videos 35.8% accessing social media 34% streaming movies
3	25 (47%)	55.9% of 34 wants to know social media updates 44.1% of 34 to contacting friends and family 20.6% of 34 to join community
4	34 (64%)	47% of 34 watching movies 5% of 34 watching anime 23% of 34 watching othes
5	32 (60%)	64% of 32 playing games 34% of 32 didn't play games
6	33 (62%)	33.3% of 33 to get social media passwords 27.3% of 33 to do DoS attacking 24.2% of 33 to do hacking computers 21.2% of 33 to do hacking websites 24% of 33
7	34 (64%)	70.6% of 34 just for fun 26.5% of 34 wants to learn more 20.6% of 34 inspired by movie scene

Based on Table 3, researcher got 2 main points that students are frequently accessed social media and searched for hacking tutorials. This isn't appropriate with school rules. A firewall with MikroTik will be used to restrict student access to that 22 main points.

C. MikroTik Script Configuration

The configuration is done in WinBox software using terminal menu. Script allows researcher to freely configure MikroTik as existing conditions [16]. The script includes basic internet configuration, blocking sites using raw and filter rule, and preventing DoS using filter rule and raw.

D. Result

First test is accessing all social media. Testing is carried out through one of the client PCs in the computer lab.

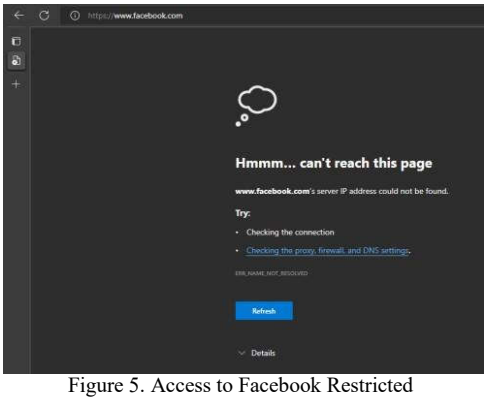

Figure 5. Access to Facebook Restricted

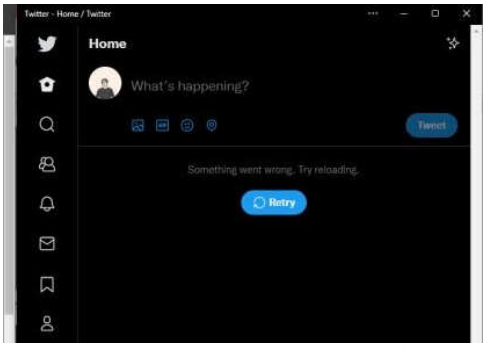

Figure 6. Access to Twitter Restricted

From the Fig. 5 and Fig. 6, social media blocking was success. Social media sites such as Facebook and Twitter can't be accessed because the MikroTik firewall block it.

The second test is accessing movie streaming sites. Result shown in Fig. 7 and Fig. 8.

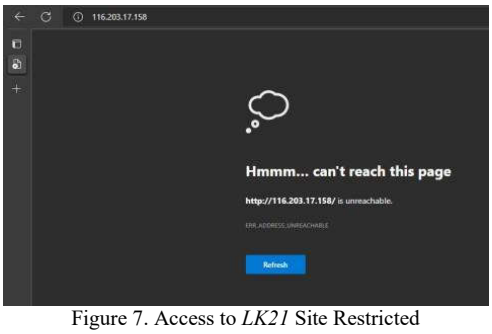

Figure 7. Access to *LK21* Site Restricted

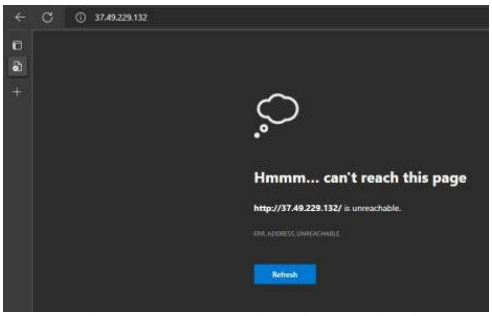

Figure 8. Access to *idlix* Site Restricted

From the Fig. 7 and Fig. 8 above, movies sites blocking was success. All of those sites can't be reached.

The last test is DoS attacking. Result shown in Fig. 9 and Fig. 10.

Figure 9. *LOIC* Software Result After Firewall Implementation

Fig. 9 shown that the client sends TCP packets to IP addresses 192.168.222.1 which is the ether5 gateway IP address but there is no packet sent, requested remains 0. This indicates that the filter successfully blocked the attacker access.

```
[admin@MikroTik] > system resource print
                   uptime: 1h20m30s
                  version: 6.47.1 (stable)
               build-time: Jul/08/2020 12:34:22
         factory-software: 6.46.3
              free-memory: 218.5MiB
             total-memory: 256.0MiB
                      cpu: MIPS 1004Kc V2.15
                cpu-count: 4
            cpu-frequency: 880MHz
                 cpu-load: 1%
           free-hdd-space: 4708.0KiB
          total-hdd-space: 16.3MiB
  write-sect-since-reboot: 455
         write-sect-total: 10859
               bad-blocks: 0%
        architecture-name: mmips
               board-name: hEX
                 platform: MikroTik
```

Figure 10. MikroTik Resource After Firewall Implementation

Fig. 10 was taken during DoS testing and shows that the hardware resource didn't go up and still in 1% as normal. This indicates that the firewall has successfully prevented DoS attacks.

IV. CONCLUSION

After doing the research and getting the results and then doing the analysis, the next step is to make conclusions from the analysis. The following are some conclusions obtained from this research.

The firewall script is formulated on the MikroTik terminal using the WinBox software. The formulation of the script is based on observations and questionnaires which produce website data that students frequently access and other things that are done. The Raw and filter features in the MikroTik firewall are used as basic parameters for blocking websites and dealing with DoS attacks.

The results of firewall testing using a combination of filters and Raw succeeded in blocking access to social media websites

and streaming movies sites. The client can't access and the client browser displays continuous loading. Firewall testing to ward off DoS attacks was also successful. When tested, LOIC didn'tsend any request packets and when CPU resources were checked, the resources were only 1%.

Based on the test results, the use of a firewall on the MikroTik router is effective in limiting access to students to other things outside of learning field. With this firewall, students are expected to be able to use the facility positively and focus more on learning.

Based on the results obtained from this study, suggestions can be given, to use another method to block websites that use dynamic public IPs, adding other actions as an such as directing clients to other websites when accessing social media, and adding other parameters to get the value from the test so that there are mathematical calculations that can be analyzed in the discussion.

REFERENCES

[1] MA Abdilah, I. Alfiani, MA Ulbarokah, and KW Nugraha, 'OPTIMIZATION OF MICROTIC ROUTERBOARDS AS AN EFFORT FOR A HEALTHY INTERNET', vol. 1, no. 1, p. 7, 2021.

[2] B. Jaya, Y. Yuhandri, and S. Sumijan, 'Improving Mikrotik Router Security Against Denial of Service (DoS) Attacks',Jsisfotek, pp. 115–123, Dec. 2020, doi:10.37034/jsisfotek.v2i4.32.

[3] IDMBA Darmawan and IGOG Atitama, 'Fundamental Mikrotik Workshop Module', Udayana University Net-Centric Computing LAB, p. 29.

[4] BILHANET, 'Social Media Content Domains: Facebook, Instagram, Twitter for Mikrotik', BILHANET, Mar. 31, 2021. https://bilhanet.com/mikrotik-content-media-social-facebook-instagram-twitter/ (accessed Aug. 15, 2022)

[5] AD Prasetyo, 'Application of Mikrotik Router-Based Wireless Network Using VTP (Vlan Trunk Protocol) Method at PT. Pertamina Asphalt Factory Gresik', Dinamika University, Undergraduate Thesis, 2017.

[6] MD Lesmana Siahaan, M. Sari Panjaitan, and AP Utama Siahaan, 'MikroTik Bandwidth Management to Gain the Users Prosperity Prevalent', IJETT, vol. 42, no. 5, pp. 218–222, Dec. 2016, doi:10.14445/22315381/IJETT-V42P243.

[7] F. Khafif and K. Semarang, 'INCREASING INTERNET SERVICES USINGMICROTIK AND WINBOX SOFTWARE AT PTIPD UIN WALISONGO SEMARANG', vol. 3, no. 1, p. 4, 2021.

[8] I. Riadi, 'Optimizing Network Security Using Mikrotik-Based Application Filtering', p.11.

[9] 'Basic Concepts of MikroTik Firewalls and Their Functions on Networks'. https://kharismaworld.co.id/blog/firewall-mikrotik (accessed Jul. 30, 2022).

[10] 'Mikrotik Indonesia on Twitter', Twitter. https://twitter.com/mikrotik_id/status/1527547197784719360 (accessed Aug. 15, 2022).

[11] T. Hart, Networking with MikroTik: MTCNA Study Guide.pdf, 1st ed. Independently published, 2017.

[12] 'MikroTik Filter Rule - Nevtik'. https://nevtik.org/mikrotik-filter-rule-part1/ (accessed Aug. 02, 2022).

[13] Z. Chao-yang, 'DOS Attack Analysis and Study of New Measures to Prevent', in 2011 International Conference on Intelligence Science and Information Engineering, Wuhan, China, Aug. 2011, pp. 426–429. doi:10.1109/ISIE.2011.66.

[14] A. Bhardwaj, A. Sharma, V. Mangat, K. Kumar, and R. Vig, 'Experimental Analysis of DDoS Attacks on OpenStack Cloud Platform', in Proceedings of 2nd International Conference on Communication, Computing and Networking, vol. 46, CR Krishna, M. Dutta, and R. Kumar, Eds. Singapore: Springer Singapore, 2019, pp. 3–13. doi:10.1007/978-981-13-1217-5_1.

[15] Dwiky and A. Aziz, 'Students' Habits When Provided with Laptop Facilities and Internet Access'.

[16] A. Yanwar Syarif and N. Mashitoh, 'School Policy Regarding Student Internet Access', Aug. 01, 2022.