Combination of Filtering and Switching Methods for Network Security from Pornographic Content

1st Yunif Lukman Hakim, 2nd Hendro Wijayanto*
Informatics Program, STMIK Sinar Nusantara
Surakarta, Indonesia
20530016.yunif@sinus.ac.id[1] , hendro@sinus.ac.id[2]

Abstract— The internet provides convenience in various aspects of human life. Internet penetration in Indonesia has grown by 66.5% of the total population of 278.7 million people. This shows that 185.3 million people are active internet users. Based on the report of the Ministry of Communication and Information (Kemenkominfo), it has handled negative content since 2016 to 2023 with a total of 1.9 million contents. With the most access through website media. MikroTikRouter Os as a tool used to support computer network communication, is expected to minimize access to this negative content. Configuration in MikroTik devices with Layer7 Protocol and Firewall Rules is used to prevent access to negative content from the client side. A firewall is a network security tool that monitors incoming and outgoing network traffic. The application layer that acts as a liaison between applications and network functions, manages how applications access the network, and regulates the creation of error messages is called Layer 7 Protocol. The Layer 7 Protocol configuration and firewall rules are effectively applied to Mikro Tik RB941-2ND to ward off negative pornographic content on local networks with a percentage of 87% of the 91 websites that have been tested. In particular, the test results show that this method is an effective scheme using unwanted travel with global internet usage and without using a Virtual Private Network (VPN). By using this filtering and switching technique, negative site access restrictions can be minimized. At least it can be a pioneer of a healthy internet.

Keywords—Networking, Mikrotik, Layer7Protocol, Firewall, Porn Site

I. INTRODUCTION

The internet provides convenience in various aspects, starting from work, teaching and learning processes, sources of information and knowledge, entertainment, places to work and everything else [1]. Based on a survey conducted by We Are Social & Meltwater and published in the Datareportal for Indonesia Overview January 2024, it shows that internet penetration has grown by 66.5% of the total population of 278.7 million people. This shows that 185.3 million people are active internet users[2].
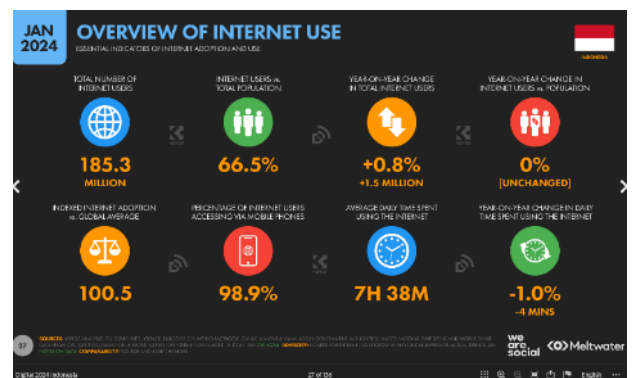

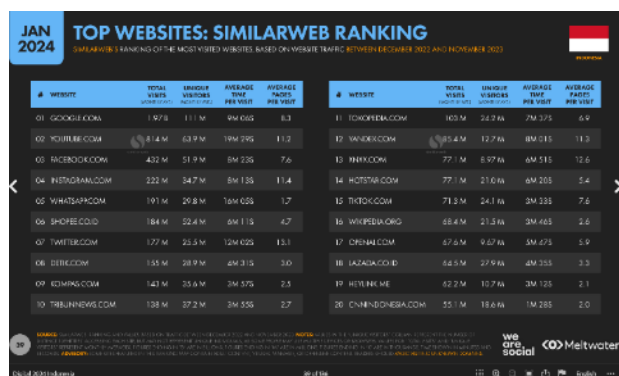Figure 1. We Are Social & Meltwater Datareportal 2024

Figure 2. Indonesia Top Website 2024

From Figure 2, it turns out that there are websites that fall into the negative website category. "Yandex" and "xnxx" occupy the 12th (twelve) and 13th (thirteenth) positions of websites that are frequently accessed by internet users. "Yandex" (or called Yet Another Indexer) is a search engine from Russia and is provided in the form of the Yandex Browser application. It supports connections with private mode (VPN). While "xnxx" is a free pornography service site.

Pornography consumption and demographic variables are interrelated. For example, personal characteristics, sensations, sexual experiences, environment, cyber habits and work. Most teenagers realize that most pornographic material is excessive and unrealistic. In addition, pornography is not only watched out of curiosity and to arouse sexual desire, but is also used as a source of sexual information, especially by minority groups. Sometimes this can become a culture and lead to deviant behavior and crime [3][4].

The internet also provides freedom for its users to access unlimited information, not all of which is positive. The influence of inappropriate content on the internet is in the form of pornography, gambling, fraud, harassment, cyberbullying, and other cybercrimes. This content should be blocked so as not to harm internet users in real life[5]. Based on the report of the Ministry of Communication and Information (Kemenkominfo), it reported that it had handled negative content from 2016 to 2023 with a total of 1.9 million contents. With the most access via website media [6]. Globally, the digitalization era has become a pandemic for society in the use of digital media, especially website content. The impact of accessing pornography is not only on the perpetrators, but can also have an effect on the community environment, especially immoral crimes[7]. Moreover, Indonesia has experienced the COVID-19 pandemic which caused all activities to be carried out online. The potential for crime is also increasing, including cases of pornography[8].

Seeing the above problems, it is necessary to impose restrictions on the computer network system in the implementation of a healthy and positive internet by utilizing the Firewall Filtering function via MikroTikRouterOs as a tool used to support work system access in this study[9]. Firewall filtering on the Mikrotik router service overcomes the above problems because firewalls can generally protect the network from the inside and outside of the router through the features provided. With the MikroTik RouterBoard service, firewalls can also limit incoming and outgoing flows through the network[10]. Because there are still many who use internet access in places such as campuses, schools and agencies that provide public spaces, the implementation of content filtering is quite efficient for filtering negative content that is worthy of being accessed.

In computer networking, switching is the process of effectively redirecting data packets from a source to a destination. To map ports and connected devices using the Media Access Control (MAC) address table. The key to switching is to divide the network into smaller parts to reduce data collisions, improve network performance and security, and manage data traffic. In addition, switches allow the use of Virtual Local Area Networks (VLANs) and access control to separate sensitive traffic, improving network efficiency and security [11]. The results of cyber attack analysis show that the use of network infrastructure really determines computer security. Overall design, development and evaluation of infrastructure can enable the development of good technology[12].

A computer network is a telecommunications infrastructure that allows two or more computer devices to communicate with each other. The main purpose of a computer network is to convey information content and services

through media. Currently, there are many network communication media and information processing media[13].

A firewall is a network security tool that monitors incoming and outgoing traffic to and from a network. Based on rules created by an administrator, its job is to determine whether a particular data packet should be accepted or rejected. A firewall serves as the first line of defense for a computer network, distinguishing a controlled local network from an external network, such as the Internet [14][15]. In a computer network, a firewall plays a very important role and acts as the primary defense to protect the network infrastructure. The increasing sophistication of attackers also heightens the threat of cyber attacks, making the firewall's role even more crucial[16].

The Layer7 Protocol (L7 Protocol) is the application layer that serves as an intermediary between applications and network functions, managing how applications access the network and regulating the creation of error messages. Protocols included in this layer are HTTP, FTP, SMTP, and NFS. Additionally, the Layer7 Protocol has capabilities such as blocking sites by adding new filter rules[17]. Filter rules are used to regulate the flow of network data, covering various criteria such as address, action, connection status, protocol, port, time, and interface. By using firewall filter rules, potentially malicious network activities can be stopped, such as restricting access to certain websites and preventing the use of applications like port scanning, VPN, Torrent, and recursive DNS [18][19].

MikroTik is a manufacturer of hardware and software for computer networking equipment, particularly router devices. Their products range from internet services, business services, to individual users. The company is based in Latvia and was founded in 1996. In 2002, the company created hardware called RouterBoard, a network device that also contains the MikroTik operating system[20].

II. RESEARCH METHODS

In this research, qualitative research methods were used. The stages in this method are identification of research topics, qualitative design, data analysis, description of research conclusions, and research reporting [21][22]. In the research topic identification stage, a literature search is carried out, reviewing related articles. For qualitative design, what is done is to collect data obtained from the Kaggle Dataset. Meanwhile, to carry out the analysis process is to configure filtering and switching on the Mikrotik RouterBoard. In the analysis process, trials are carried out on the success of the filtering and switching processes. After these stages, reporting and assessment of the analysis results are carried out.

The data needed in this research process is URL data or word expressions that fall into the category that will be filtered. Data is taken from the Kaggle Dataset with the dataset name "URL Classification". Which in the dataset there are 35190 URLs with the Adult category.

In the case of this research, using the Mikrotik RouterBoard RB941-2ND device. This is because this device is easy to obtain and is often used by the public. Network security against pornographic content uses two methods combined to obtain optimal results. Filtering and switching methods are used in this study. The process flow of using the filtering and switching methods is shown in Figure 3:
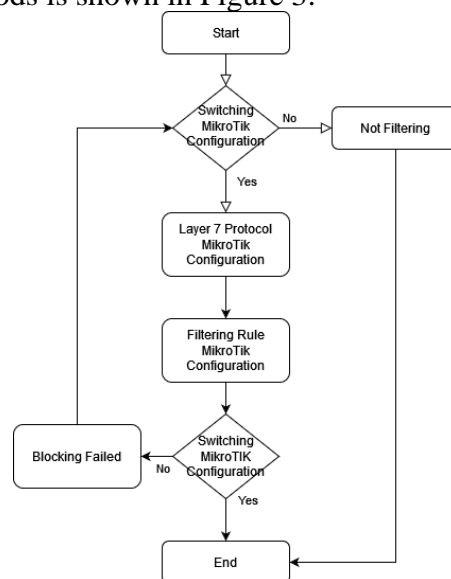

Figure 3. Flowchart Filtering and Switching

The process begins with the configuration of the switch on MikroTik to manage network

traffic, followed by the setting of firewall filter rules which include creating rules to block pornographic content using Layer7 Protocols. Once the rules are set, the connections and filters are tested to ensure their effectiveness. If the filter successfully blocks pornographic content, the next step is continuous monitoring and adjustment to ensure the system continues to function optimally. If it fails, the firewall configuration is adjusted again. The process ends when the filtering system is successfully implemented and verified to be running as needed.

A. Layer7 Protocol Configuration

In Layer7 Protocol configuration involves setting parameters that allow control and management of network traffic at the application level. This process includes the creation of rules to regulate application access to the network, such as setting security policies, determining data traffic priorities, and implementing content filters with certain keywords. The formula or procedure for writing regexp (regular expression) is as below :

```
regexp:^.+(keyword1|keyword2|keyword3
|keyword4|…etc).*\$
```
----- (1)

Writing regular expressions (regex) like this to ensure that the checked string has one of the specific keywords anywhere in the string, and matches the entire string from the beginning (**^**) to the end (**$**). There are no limitations for writing keywords, according to your needs. You can add any keywords about the content, contents, information, to the writing you want to filter..

B. Firewall Rule Configuration

Firewall rule is a basic firewall in MikroTik to block traffic that matches the Layer7 Protocol rules. To configure MikroTik using the following rules:

```
/ip firewall filter add chain =
fitur-manglelayer7-protocol        =
name(as    made)action=     firewall-
rulescomment = "your-comment"
```
----- (2)

Information :
- There are 5 (five) mangle features in the chain, namely: input, output, forward, prerouting and postrouting.
- There are 7 (seven) features in the firewall

rules, namely: accept, drop, jump, reject, tarpit, passthrough and log.

This firewall rule ensures that all traffic containing the domains in the regular expression (regex) will be blocked. Firewall rules are arranged in sequential chains. Each packet will be matched against the criteria in a chain. If there is a match, the packet will be executed. However, if the incoming packet does not match, it will be rushed to the next rule until it matches.

C. Network Topology

In this study, the network infrastructure uses a topology involving the RouterBoard RB941-2ND device that supports wired and wireless connections. The network topology consists of an internet connection connected to the RouterBoard RB941-2ND for content management and filtering. Then forwarded to the switch that connects user devices such as personal computers (PCs), notebooks/netbooks, and smartphones. The MikroTik router is configured with NAT, Filter rule, and uses Layer7 Protocol for in-depth inspection and content blocking based on data patterns. This is intended to ensure that all devices get filtered and secure internet access through centralized settings on the MikroTikRouterBoard RB941-2ND.
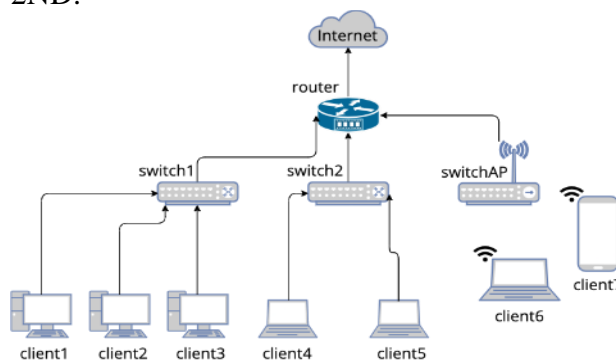

Figure 4. Network Topology

D. Analysis and Testing

In the test, it was done by analyzing the results of the implementation of layer 7 protocol and firewall rules on access to pornographic sites / prohibited sites. The analysis was seen from the level of success of the execution test in filtering.
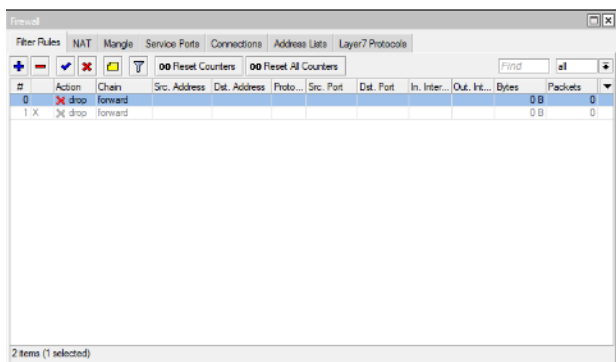
III. RESULT AND ANALYSIS

In the case of this research, using the Mikrotik RouterBoard RB941-2ND device. This is because this device is easy to obtain and is often used by the public. Filtering and switching methods are implemented by utilizing MikroTik RB941-2ND on a local network scale. Client access uses wired and wireless network connections with various types of devices (computers, laptops, smartphones and smartphones/tablets).

A. Layer7 Protocol Implementation

Regular expressions in the layer 7 protocol configuration are specifically designed for the expression of information or data that is pornographic in nature. The addition of regular expressions (regex) aims to check and block network content based on certain text patterns that appear in data traffic, such as URLs (Uniform Resource Locators) or content in HTTP (Hypertext Transfer Protocol (HTTP) packages.

The URL and HTTP data used in the regular expression are referenced from the URL Classification downloaded from the Kaggle Dataset with the Adult category. From these results, frequently occurring words are classified and visualized using wordcloud. The results of the wordcloud visualization from the Kaggle URL Classification Dataset are shown in Figure 5

Figure 5. Wordcloud URL

This Wordcloud URL is used in the implementation of regular expressions (regex) in the firewall layer 7 protocol in MikroTik. Writing regular expressions using formula number 1 above, with the following results:

```
^.+(porn|geocities|s*x|ang*lf*re|p*rn|
l*sb*an|g*y|h*rdc*re|x*x|am*teur|p*ssy|
ad*lt|n*de|s*xy| er*t*ca).*\$
```
some words are hidden for the reader's convenience

Regular expression (regex) configuration is done on MikroTik by selecting the **IP - Firewall - Layer7 Protocols** menu and entering the expression in the **Regexp** section. The configuration is as in Figure 6

Figure 6. Regex Layer7 Protocol

MikroTik will detect and block access to websites that have certain characteristics according to the expression written in the Regexp Layer 7 Protocol. From the results of filtering in this Layer7 Protocol, if the user accesses information containing the word, it will be forwarded to the firewall rules, otherwise the user will get the desired website information.

B. Firewall Rules Implementation

This Firewall Filter rule is set in a chain forward to capture traffic passing through the router. On the Advanced tab, the Layer7 Protocol that has been created contains sites that will be blocked. On the Action tab, set the drop action to block access to the site. With this step, all traffic directed to the address in the address list (Regexp) will be stopped, thus blocking access to blocked sites. The configuration can be shown in Figure 7

Figure 7. Firewall Filter Rule

C. Testing and Analysis Result

In the testing process, MikroTik RouterBoard RB941-2ND is used and implemented to handle several computer laboratories as well as several laptop and smartphone devices. The testing process uses execution tests in filtering and switching configurations. This test is done by directly accessing websites that are categorized as pornography on each client. In this test, it is not limited to the type of browser used. If MikroTik successfully blocks the site accessed by the client, then the status of the website display on the client is in a drop condition, or as in Figure 8
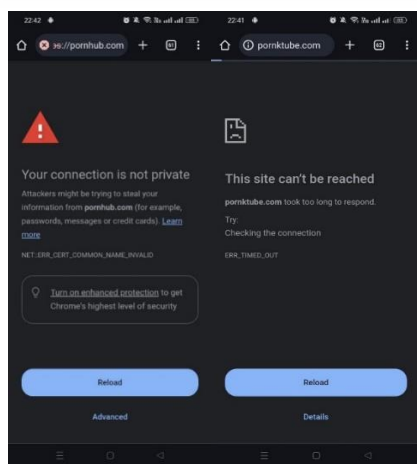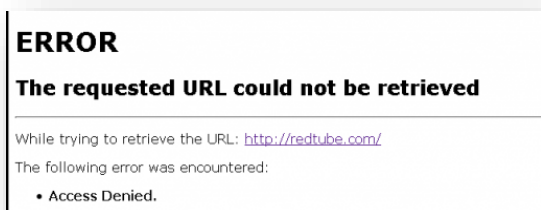
Figure 8. View of Blocked Websites Accessed

Of the several website displays that are included in the filtering layer 7 protocol, some are not immediately blocked. Websites will sometimes enter "connection is not private" mode. If the user forces entry with the "Advanced" facility, the user will still get a display that the website cannot be accessed.

From the trials conducted, the test used a sample of 91 URL tools / websites that potentially contain pornographic content. The samples used range from streaming service providers, artificial intelligence content (AI Content), and story or comic services.

Table 1. Test Result

No	URL / Sites	Status
1	bra**ers.com	Blocked
2	b*ngb*os.com	Blocked
3	real*tyk*ngs.com	Blocked
4	sp*cev*ds.com	Blocked
5	ikn*wthatg*rl.com	Blocked
6	ad*ltt*me.com	Blocked
7	pur*tab*o.com	Blocked
....	....	....
....	....	....
64	l*nd.mu*h.ai	Unblocked
65	de*pm*de.ai	Unblocked
66	ang*lg*.ai	Unblocked
....	....	....
....	....	....
88	l*vr.ai	Unblocked
89	p*r*joy.ai	Blocked
90	*wa*fu.com	Blocked
91	n*nol*.ai	Blocked

* accessed using global connection and without VPN
*some words are hidden for the reader's convenience

The trial was conducted on several client devices connected to MikroTik RB941-2ND with filtering and switching configurations. From Table 1 above, there are still several URLs or websites that have not been successfully blocked. The results of the trial between websites that were successfully blocked and failed to block are as shown in the diagram in Figure 9.
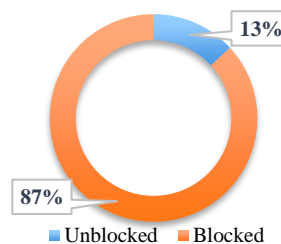

Figure 9. Diagram Result

Of the 91 website addresses used for the trial, 79 websites (87%) were successfully blocked, while 12 websites (13%) addresses escaped MikroTik filtering and switching. From the analysis results, currently many website content media minimize words containing pornography, so there are still some that escape the firewall filtering. Even content that is not successfully blocked also escapes the security of Positive Internet Indonesia if using certain internet providers. From the results of the trials conducted, it can be concluded that the use of firewall rules and Layer7 Protocol in MikroTik can block pornographic content websites with an effectiveness rate of 87%.

IV. CONCLUSION

This study shows that the Layer7 Protocol configuration and firewall rule are effectively applied to MikroTik RB941-2ND to block negative pornographic content on the local network with a percentage of 87% of the 91 websites that have been tested. Specifically, the test results show that this method is an effective scheme using unwanted travel with global internet usage and without using a Virtual Private Network (VPN). The results of this research prove that filtering and switching implemented in the MikroTik RouterBoard RB941-2ND is quite effective for blocking negative sites.

Further research can use scheduling time if necessary to determine free internet usage at certain hours. As well as switching management to make it easy to use for larger network scales. Identification of each website so that it can be used in the filtering expression reference also needs to be done so that the configuration is more effective.

ACKNOWLEDGMENT

REFERENCES

[1] R. Kurniawan *et al.*, "Penggunaan Internet yang Sehat dan Aman di Kalangan Masyarakat dan Pelajar," *Jurnal ABDIMASA Pengabdian Masyarakat*, vol. 4, no. 2, pp. 15–21, 2021.

[2] We Are Social & Meltwater, "Digital 2024 Global Overview Report," https://datareportal.com/reports/digital-2024-global-overview-report.

[3] F. W. Paulus, F. Nouri, S. Ohmann, E. Möhler, and C. Popow, "The impact of Internet pornography on children and adolescents: A systematic review," *Encephale*, 2024, doi: 10.1016/j.encep.2023.12.004.

[4] S. Prantner *et al.*, "Female Affective Perception of Mainstream and Paraphilic Pornography: Associations with Sexual and Psychological Intrapersonal Variables," *Arch Sex Behav*, vol. 53, no. 2, pp. 715–733, Feb. 2024, doi: 10.1007/s10508-023-02701-8.

[5] Dr. Aneu Yulianeu dan Oktamala, "Jurnal Teknik Informatika Atmaluhur," *Jurnal Teknik Informatika Atmaluhur*, vol. 6, no. 1, p. 40, 2022.

[6] Nabilah Muhamad, "Kominfo Blokir 1,9 Juta Konten Pornografi di Internet RI, Terbanyak dari Website," https://databoks.katadata.co.id/datapublish/2023/09/19/kominfo-blokir-19-juta-konten-pornografi-di-internet-ri-terbanyak-dari-website.

[7] M. Asbari and B. Isnawati, "Pornografi dan Pengasuhan Anak: Menganalisis Dampak Media Digital terhadap Peran Keluarga dan Perkembangan Anak," *Journal Of Information Systems And Management*, vol. 03, no. 01, 2024, [Online]. Available: https://jisma.org

[8] H. Wijayanto and I. A. Prabowo, "Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 3,

pp. 395–399, Nov. 2020, doi: 10.32736/sisfokom.v9i3.1021.

[9] C. K. Wilujeng *et al.*, "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik," vol. 8, no. 3, pp. 2680–2685, 2024.

[10] A. Jamalul'ain and O. Nurdiawan, "Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik (Studi Kasus: CV. Mitra Indexindo Pratama)," *Jurnal Mahasiswa Teknik Informatika)*, vol. 6, no. 2, pp. 560–570, 2022.

[11] H. Zhahir and M. Ardhiansyah, "Implementasi Manajemen Bandwidth Dengan Menggunakan Metode Load Balancing Dan Failover Pada Router MikroTik Dan Switch Cisco (Studi Kasus: Pusat Penguatan Dan Pemberdayaan Bahasa Kemdikbud Ristek)," *Informatika*, vol. 3, no. 2, pp. 176–193, 2022.

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

[13] R. et al. Setiawibawa, *Jaringan Komputer*. Eureka Media Aksara, 2023.

[14] A. B. Pratomo, "Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros Developing a Firewall System on a Computer Network Based on Mikrotik Routeros," *Bulletin of Network Engineer and Informatics (Bufnets)*, vol. 1, no. 2, pp. 51–59, 2023, [Online]. Available: https://doi.org/10.59688/bufnets

[15] W. Hidayat M and A. D. Yusuf, "Manajemen Penjadwalan Waktu Blokir Akses Internet pada Mikrotik RouterOS," *Journal of Security, Computer, Information, Embedded, Network, and Intelligence System*, vol. 8329, pp. 10–15, 2023, doi: 10.61220/scientist.v1i1.232.

[16] R. S. , Yadav and P. , Likhar, "Firewall: A Vital Constituent of Network Security, in Information Technology Security: Modern Trends and Challenges," *Singapore : Springer Nature Springer*, pp. 47–67, 2024.

[17] J. Kridatama and S. Dan Teknologi Penerapan, "Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router Mikrotik," 2023.

[18] U. Radiyah, "Optimalisasi Keamanan Wide Area Network (WAN) Menggunakan Raw Firewall Berbasis Mikrotik pada PT. Permata Graha Nusantara," *INTI Nusa Mandiri*, vol. 17, no. 1, pp. 16–23, Aug. 2022, doi: 10.33480/inti.v17i1.3401.

[19] M. Ali and F. Latifah, "Implemenasi Block Access Pengguna Layanan Internet Dengan Metode Filter Rule Dan Layer 7 ProtocoL," vol. 5, no. 2, 2021, doi: 10.52362/jisamar.v5i2.

[20] Mikrotik, "About us and Company Profile," https://mikrotik.com/aboutus.

[21] J. L. Johnson, D. Adkins, and S. Chauvin, "Qualitative Research In Pharmacy Education A Review of the Quality Indicators of Rigor in Qualitative Research."

[22] M. Hennink and B. N. Kaiser, "Sample sizes for saturation in qualitative research: A systematic review of empirical tests," *Soc Sci Med*, vol. 292, Jan. 2022, doi: 10.1016/j.socscimed.2021.114523.