Bit-Tech

Vol.5, No.2, December 2022
Available online at: http://jurnal.kdi.or.id/index.php/bt

Implementasi Malware Security and Proxy Layer 7 Protocol at Routerboard Mikrotik

Intan Kumalasari[1)*], Aswin Yadi Saputra[2)]

Jurusan Teknik Informatika, Fakultas Ilmu Komputer Universitas Pamulang
Jl. Surya Kencana No. 1, Pamulang – Tangerang Selatan, 15417, Indonesia

[1)]Dosen02368@unpam.ac.id
[2)] Aswinyadi@gmail.com

Article history:

Received 18 Nov 2022;
Revised 30 Nov 2022;
Accepted 13 Dec 2022;
Available online 14 Dec 2022

Keywords:

Malware
Proxy Server
Microtik
Media Social
Keyword

Abstract

In today's era along with the times, the internet network is needed in finding information because the internet is used as a source of information and exchange data in real time. Therefore, the internet is used in daily human activities, especially in the world of education. In the world of education, the internet is usedas a means of online learning and as a source for finding learning materials related to education. In an educational institution, the number of users connected to the internet network is very large, making it possible for infiltration by malware and distribution. Malware activity is closely related to computer memory, computer performance and also network activity on computer systems making it difficult to access learning media sites in the network because there is no network security management that regulates the data exchange traffic of each user. The right solution to overcome this problem is to implement malware security and proxy server configurations as the method used to manage traffic for data exchange activities. The methodology used is dynamic analysis by analyzing malware on a system and looking at the activities or processes activated by the malware. By applying the security malware method and proxy server configuration, the quality of the network will be better because it minimizes malware traffic on the network system according to the configuration that is applied and also users will be restricted from accessing certain sites.

I. INTRODUCTION

Education is basically an effort to create a learning process and a planned learning atmosphere so that students actively develop personal potential to have personality, noble character, self-control, intelligence, religious spiritual strength, and have skills that will later be useful for themselves. and society in the future.

In supporting developments in the world of education, technology and information are needed to support teaching and learning activities in schools. In using information technology, there are definitely advantages and disadvantages. One of the advantages of technology and information in the world of education is that it makes it easier to find information related to learning and increases the ability of pupils and students to utilize technology and information at school. However, the drawback of technology and information is that it is easy for students and female students to access information that is not related to teaching and learning activities so that students and students do not understand the material presented by teachers during teaching and learning activities.

Malware (Malicious Software) is a program designed with the aim of infiltrating a computer system, which will damage the computer system. Malware can enter many computers via internet networks such as email, downloads from the internet, or through infected programs. Malware can cause damage to computer systems and also enable data/information theft.

A proxy server is a server that is placed between a client application and the server application being contacted[12]. This server is used for filtering and monitoring data packets from the internet network which will later be forwarded to the local network. With this server, at least it minimizes data packets that are not needed by the client and is also one way to increase network security.

Students often access sites that are not related to teaching and learning activities during practicums using computers connected to the Al- Wildan Islamic School 3 BSD internet network via cable or wireless.

Therefore, the author is interested in conducting research on "Implementation of Malware Security and Proxy Layer 7 Protocol on Mikrotik Routers"

[*] Corresponding author

doi: 10.32877/bt.v5i2.953

II. Related Works/Literature Review (Optional)

The first research was conducted by Md Rifat Bin Emdad and Md Shahun Khan, students of the Computer Science and Engineering study program at Jahangirnagar University (2019) A Stardard Data Security model Using AES Algorithm in Cloud Computing. In their research, researchers analyzed data security through Cloud Computing" [2] which discusses data security standards in cloud computing using the AES algorithm method. Here, AES security is guaranteed by implementing a good key management system and a well-developed structure. This model can be applied on various cloud computing platforms to get a more efficient way of cloud computing like SaaS, PaaS etc.

The second research was conducted by Rinto Erlando, Diana Diana and Maria Ulfa (2018) conducted research on the Implementation of Firewall Security Systems on Cisco 1841 Routers and Monowalls on the BSD Operating System (Berkeley Software Distribution [4] which discussed Primary Data Collected directly from the object under study, using the Firewall and Monowal methods with the results of DDoS attack trials using the Firewall security system on the CISCO 1841 router with 10 attempts, the results were 6 failed attempts to enter and 4 successful attempts to enter using the Firewall security system using Firewall and monowall methods.

The third research was carried out by [6] who conducted research on Comparative Analysis of Mikrotik Site Filter Using Address List Techniques, Layer 7 Protocols, Web Proxy, Mangle and Static DNS which discussed methods that can be used to filter data packets to certain sites using RouterOS Mikrotik, then carried out an analysis of the effectiveness of site filtering using site filtering methods provided by RouterOS Mikrotik, including the Address List Method, Layer 7 Protocols Method, Web Proxy Method, Mangle Method and Static DNS Method. By carrying out site filtering, it is hoped that it can improve the quality of network services in every company that uses the internet in its daily activities.

III. Methods

In preparing this writing, the researcher applied research methods to obtain the data needed so that the writing could be completed well. The research methods that the author carried out are as follows:

A. Identify the Problem

The author made direct observations at the location of the research object to find out what needs to be done and will be done regarding problem solving. In the previous network there was no malware and proxy security configuration because the network device used did not have features for configuring malware and proxy security. At this stage the author makes observations and then formulates the problem and appropriate solutions.

B. Needs Analysis

This stage is carried out for the hardware and software requirements that will be used, which will be implemented according to the needs and solutions to problems that exist at the location of the research object.

C. Design Planning

At this stage the author designs the proposed network topology in the form of cabling layout, network flow from the internet source to the user as a clear picture of the network infrastructure that will be implemented. This stage was carried out after the author obtained data from observations at the location of the research object.

D. Infrastructure Development

After the design process, then develop the proposed network infrastructure by creating a topology as a network scheme that will be implemented in accordance with the stages in the Network Development Life Cycle (NDLC) method.

E. Network Simulation

This stage is the process of carrying out network simulations using supporting software such as CiscoPacket Tracer to ensure the network is connected properly according to the design that has been made.

F. Configuration Implementation

After the simulation stage, we then implement the design that has been created by configuring the hardware used in this research.

IV. RESULTS

The author carried out network analysis and design before proceeding to the implementation stage of malware security management and proxy configuration to optimize quality of service using RouterBoard RB750r2. This network device is used as a replacement for existing wireless routers and already has features for configuring firewall and proxy layer 7 protocol settings. The following is the proposed network scheme proposed by the author

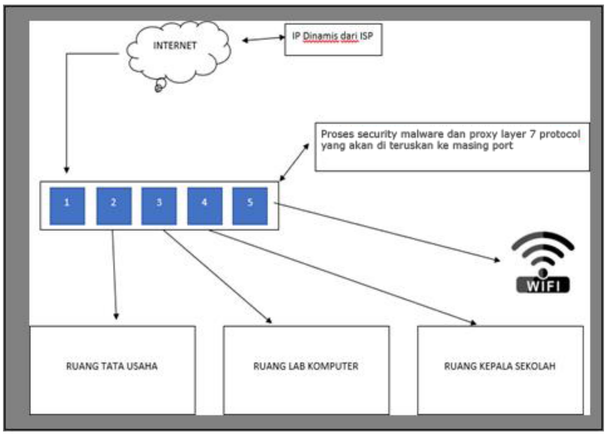


Figure 1. Proposed Network Scheme

In Figure 1, it is a network schematic of the firewall filtering management process from the ISP with an IP address that is given dynamically by the ISP and then connected to port 1 on the routerboard. On the routerboard, firewall filtering and layer 7 proxy protocols are configured according to needs which will be forwarded to each available port on the routerboard.

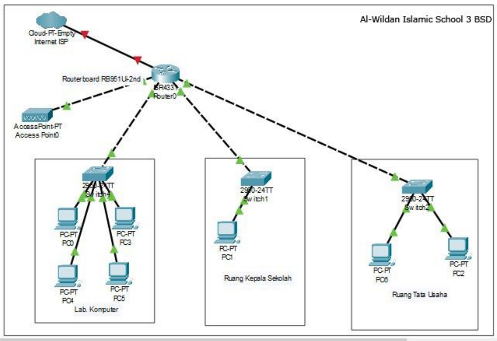


Figure 2. Proposed Network Topology Design

The topology that the author proposes in this research uses a hybrid topology, which is a combination of several topologies commonly used for local networks, including star topology and tree topology. The application of this hybrid type of topology is intended to anticipate that if one day a network problem occurs, it can be resolved quickly and precisely so that it does not interfere with other network activities because with this network topology it has a central path division in each room in the form of a hub which has one internet source cable from the routerboard which then distributed to devices in the target room. The following is the proposed network topology design that the author will apply to the network at Al-Wildan Islamic School 3 BSD. The design that will be used is as in Figure 2 above:

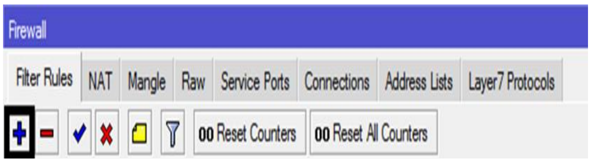
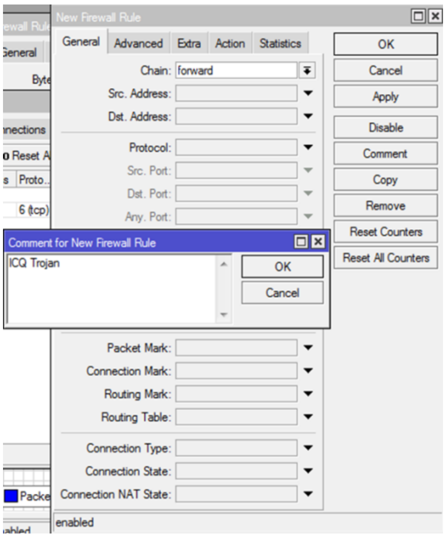


Figure 3. Adding new Filter Rules

After entering the Filter Rules menu, click the add (+) button -> After entering the New Firewall Rule menu in the Comment menu, fill in the name Malware=ICQ Trojan, then Apply -> OK



New Firewall Rule

Chain: forward

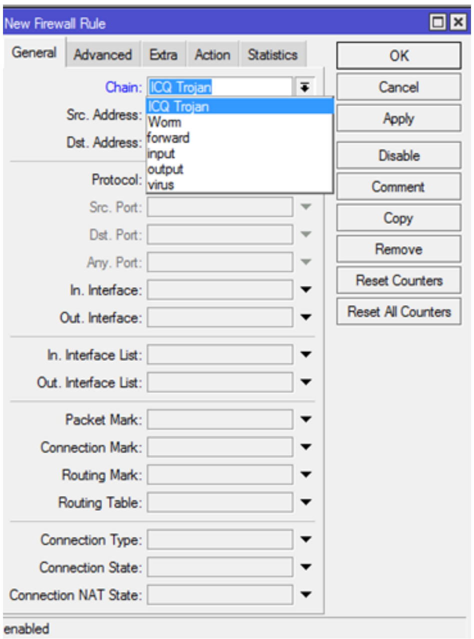
Comment for New Firewall Rule

ICQ Trojan

enabled

Figure 5. Adding Comments to Firewall rules for Malwar security

On the Comment tab, we add information or can customize it with the name of the malware. Then on the chain menu, select what is written in the Comment menu, chain = ICQ Trojan. The firewall rule display can be seen in Figure 5



New Firewall Rule

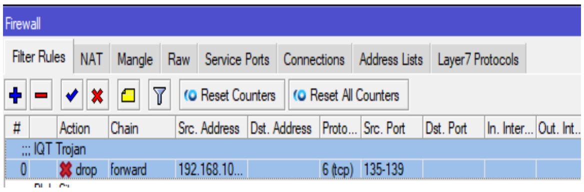
Chain: ICQ Trojan

- ICQ Trojan
- Worm
- forward
- input
- output
- virus

enabled

Figure 6. Chain selection

In this chain menu, we select the Malware name or according to what we wrote in the command menu. On the Protocol menu, enter tcp, protocol -> tcp. because this type of malware runs on the TCP protocol. The chain selection display can be seen in Figure 6.

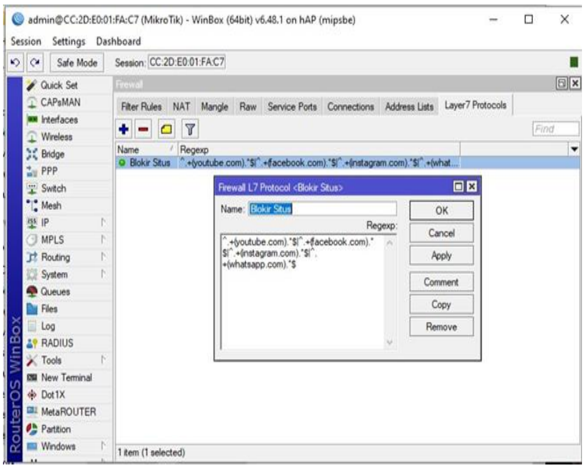


Firewall

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
::: IQT Trojan										
0		✗ drop	forward	192.168.10...		6 (tcp)	135-139			

Figure 7 Results of Malware Firewall Settings on Mikrotik

After all the malware lists have been added to the firewall rules, a list of blocked malware ports will appear in the Rules filter menu. The results of the settings will be seen in Figure 7 above. Meanwhile, adding malware rules with ports and various other types of malware can be studied and obtained from various other sources because the number of malware and ports continues to increase. The display of malware security results on the firewall can be seen in Figure 7.



Name	Regexp
Blokir Situs	^.+(youtube.com).*$\|^.+(facebook.com).*$|^.+(instagram.com).*$|^.+(what...

1 item (1 selected)

Firewall L7 Protocol <Blokir Situs>

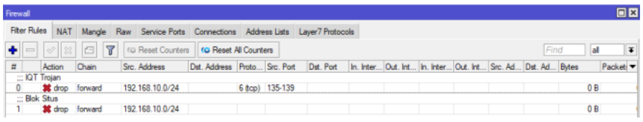
Name: Blokir Situs

Regexp:

```
^.+(youtube.com).*
$|^.+(instagram.com).*$|^.
+(whatsapp.com).*$
```

Figure 8. Layer 7 firewall protocol configuration display for site filtering

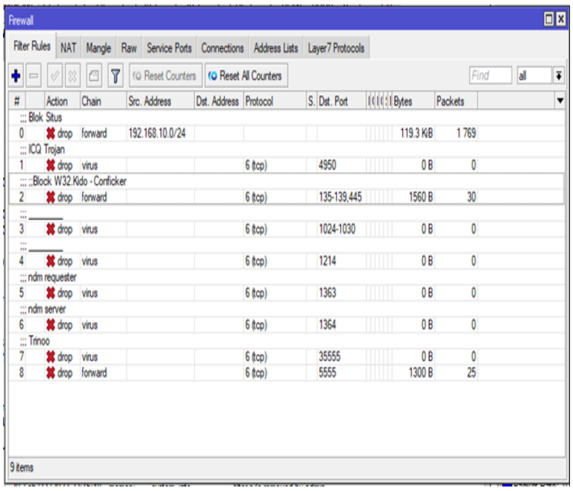
configure Layer 7 Protocols which functions as website filtering so that clients cannot access several sites that have been blocked on the routerboard. To add a site to be blocked, there are steps that need to be taken, including selecting the Layer 7 Protocols tab in the firewall feature then selecting the "+" sign and a text box will appear. In the name section, fill in the name of the site you want to block, and in the Regexpn section, fill in the following command ^.+(youtube.com).*$|^.+(facebook.com).*$|^.+(instagram .com).*$|^.+(whatsapp.com).*$| ^.+(detik.com).*$| .This command is used to block Youtube, Facebook, Instagram, Whatsapp, and detik sites. The site filling display can be seen in Figure 8.



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
::: IQT Trojan															
0	drop	forward	192.168.10.0/24		6 (tcp)	135-139								0 B	
::: Blok Situs															
1	drop	forward	192.168.10.0/24											0 B	

Figure 9. Display of firewall settings results on Mikrotik

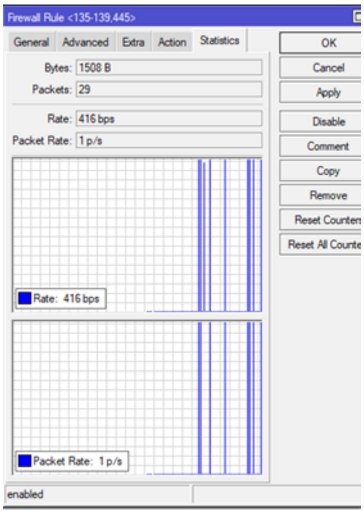
The display of the results of the layer 7 firewall protocol block site configuration can be seen in Figure 9.
A. Malware Security Testing



#	Action	Chain	Src. Address	Dst. Address	Protocol	S.	Dst. Port	Bytes	Packets
::: Blok Situs									
0	drop	forward	192.168.10.0/24					119.3 KiB	1 769
::: ICQ Trojan									
1	drop	virus			6 (tcp)		4950	0 B	0
::: ::Block W32.Kido - Conficker									
2	drop	forward			6 (tcp)		135-139,445	1560 B	30
:::									
3	drop	virus			6 (tcp)		1024-1030	0 B	0
:::									
4	drop	virus			6 (tcp)		1214	0 B	0
::: ndm requester									
5	drop	virus			6 (tcp)		1363	0 B	0
::: ndm server									
6	drop	virus			6 (tcp)		1364	0 B	0
::: Trinoo									
7	drop	virus			6 (tcp)		35555	0 B	0
8	drop	forward			6 (tcp)		5555	1300 B	25

9 items

Figure 10. Display of filter rules working on the firewall



Bytes: 1508 B
Packets: 29
Rate: 416 bps
Packet Rate: 1 p/s
Rate: 416 bps
Packet Rate: 1 p/s

Figure 11. Traffic Filter rules display

At this stage, the author tested the malware security that had previously been configured on the RB750r2 routerboard with the aim of finding out whether the configuration was running well or not.

The results that have been studied can mean that there is malware on some of the computer devices used. To see statistics on malware that exists or passes through the network, you can see the statistics menu tab in the Filter rules that have been created for malware security. The display of malware activity can be seen in Figures 10 and 11.

A. Layer 7 Protocol Filtering Testing

At the proxy filtering testing stage, the site that will be blocked is Youtube by displaying the Youtube site page before and after applying the Layer 7 Protocols method. The following are the results obtained at this testing stage

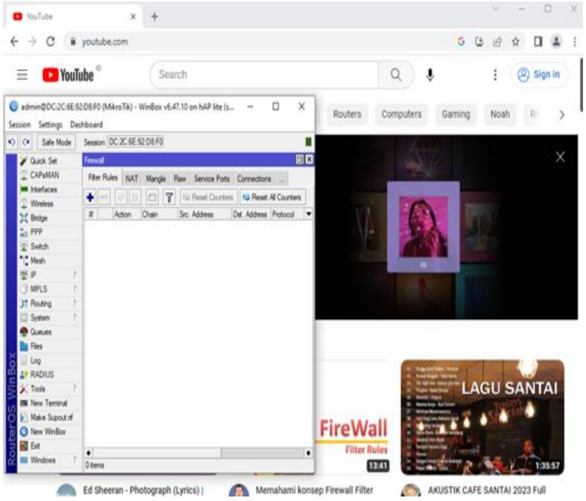
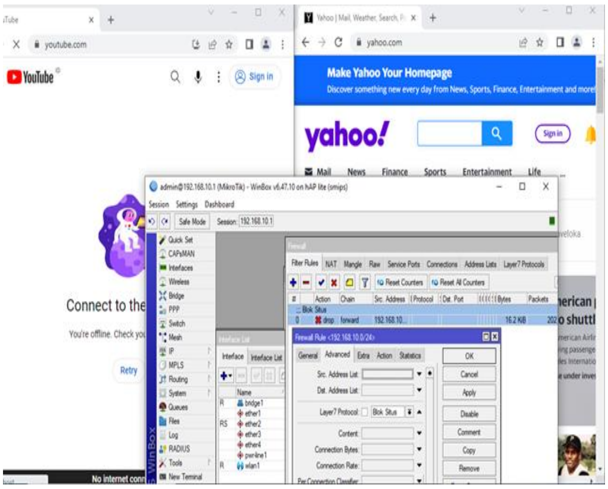


Figure 12. Testing before using the layer 7 firewall proxy protocol



Connect to the
You're offline. Check yo
No internet conn

admin@192.168.10.1 (MikroTik) - WinBox v6.47.10 on hAP lite (smips)
Session: 192.168.10.1

#	Action	Chain	Src. Address	Protocol	Dst. Port	Bytes	Packets
;;; Blok Situs							
0	drop	forward	192.168.10...			16.2 KiB	202

Firewall Rule <192.168.10.0/24>
Layer7 Protocol: Blok Situs

Figure 13. Testing before using the Layer 7 proxy protocol

At this stage, testing is carried out on accessing the YouTube site before implementation of the layer 7 firewall proxy filtering protocol is implemented. When the user wants to access the YouTube site, there are no obstacles at all in accessing the site. after activating the filter rule used to block the YouTube site. When a user wants to access the YouTube site, a page will appear as if they don't have an internet connection. This is because the Layer 7 Protocols configuration in the Filter Rule has been activated so that request data packets from the user to the server will go through filtering first. Before appearing like the image above, the characteristics that appear are when after typing in the URL address, the page requested by the user does not appear immediately but must wait for the data request process and if the process takes too long a page will appear explaining that the site cannot be accessed. The appearance of the site block firewall rule can be seen in Figures 12 and 13.

V. Discussion

The result of this research is a Security Malware to prevent network access by unauthorized users or users connected to the network using the firewall filtering method on MikroTik thereby blocking unwanted traffic. From the results of testing that has been carried out on the software, it can be said that the system can run well.

VI. Conclusions

Based on the results of analysis, design and implementation of Security Malware and proxy server configuration at Al-Wildan Islamic School 3 BSD, this research can be concluded as follows:

1) In optimizing the quality of internet network security at Al Wildan Islamic School 3 BSD, implementing Malware Security is one effective way to prevent unauthorized network access by users or users connected to the network using the firewall filtering method on MikroTik so as to block unauthorized traffic. desired.
2) In limiting site access during learning, the proxy server method is the right method for restricting students and girls from accessing sites that are not related to teaching and learning activities using the layer 7 protocol on MikroTik so that access to certain websites will be limited to each computer used students and students in the computer laboratory.

Suggestion

Based on the conclusions drawn from this research, the author hopes that this research can be continued and developed by further researchers in the future. Some suggestions from the author include:

1) To optimize security from malware attacks, you can add firewall hardware which is functionally for security and hopefully this test can be further developed for students and can be a guide for students who choose a final assignment regarding malware security on Mikrotik.
2) In this research, there are no restrictions on internet users who can connect to the network using hotspot user logins
3) In this research, the proxy server configuration used is the layer 7 protocol. The author hopes that in the future the proxy server used will use another method that is more effective than the previous method.

REFERENCES

[1] Amarudin. 2018. “Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik Router Menggunakan Metode Port Knocking.” *Seminar Nasional Sains dan Teknologi 2018*: 1–7.

[2] Bin Emdad, Md Rifat, and Md Shahin Khan. 2019. “A Standard Data Security Model Using AES Algorithm in Cloud Computing.” *International Journal of Software & Hardware Research in Engineering* 7(5).

[3] Erick. 2016. “Klasifikasi Malware Trojan Ransomware Dengan Algoritma Support Vector Machine (SVM).” 2(1): 122–27. http://ars.ilkom.unsri.ac.id.

[4] Erlando, Rinto, D Diana, and Maria Ulfa. 2020. “Penerapan Sistem Keamanan Firewall Pada Router Cisco 1841 Dan Monowall Pada Sistem Operasi Bsd (Berkeley Software Distribution).” *Bina Darma …*: 236–43. https://conference.binadarma.ac.id/index.php/BDCCS/article/view/1010.

[5] Firdaus, Mochammad, Agung. 2011. “Mengenal Berbagai Jenis Malware Dan Pencegahannya.” *Information Security*: 5.

[6] Hidayat, Arif. 2018. “Comparative Analysis of Mikrotik Site Filter Using Address List Techniques, Layer7 Protocols, Web Proxy, Mangle and DNS Static.” *International Journal of Engineering and Technology(UAE)* 7(3.4 Special Issue 4): 272–75.

[7] Kurniawan, Heru, Joseph Dedy Irawan, and F.X Ariwibisono. 2020. “Implementasi Squid Proxy Pada Mikrotik Dan Monitoring Traffic Jaringan Berbasis Website.” *JATI (Jurnal Mahasiswa Teknik Informatika)* 4(2): 136–43.

[8] Maulana, Muhammad Sony, and Muhammad Ryansyah. 2018. “Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2.” *Jurnal Sistem dan Teknologi Informasi (JUSTIN)* 6(3): 112.

[9] Noor Asyikin, Arifin, Noor Saputera, dan Edi Yohanes, and Staf Pengajar Jurusan Teknik Elektro Politeknik Negeri Banjarmasin Ringkasan. 2013. “Sistem Manajemen Hotspot Di Politeknik Negeri Banjarmasin Menggunakan Mikrotik Router Os.” *Poros Teknik* 5(1): 31–35. https://ejurnal.poliban.ac.id/index.php/porosteknik/article/view/18.

[10] Ontoseno, R Dion Handoyo, Muhammad Nurul Haqqi, and Moch. Hatta. 2017. “Limitasi Pengguna Akses Internet Berdasarkan Kuota Waktu Dan Data Menggunakan Pc Router Os Mikrotik.” *Teknika: Engineering and Sains Journal* 1(2): 125.

[11] Prama Wira Ginta, G. Putra Kusuma, E. Kusuma Negara. 2013. “ISSN : 1858-2680.” 9(2).

[12] Putra, Eka, and Arifin. 2019. “Web Proxy Server Linux Debian 8 Jessie Untuk Blokir Situs Pada SMK Al-Washliyah Pasar Senen Kota Medan Provinsi Sumatera Utara.” *Jurnal Ilmiah Core IT* (x): 1–12.

[13] Sondakh, Glend, Meicsy E I Najoan, and Arie S Lumenta. 2014. “Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat.” *Jurnal Teknik Elektro dan Komputer* 3(4): 19–27.

[14] Syarif, Abdusy, Afrius Setiawan, and Achmad Kodar. 2008. “H-1 QUALITY OF SERVICE (QoS) TEKNOLOGI STREAMING UNTUK APLIKASI SURVEILLANCE.” *Seminar Nasional Aplikasi Teknologi Informasi* 2008(Snati): 1907–5022.

[15] Syarifudin, Akhmad. 2019. “Konfigurasi Routing.” : 1–7.

[16] Tedyyana, Agus, and Supria Supria. 2018. “Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway.” *INOVTEK Polbeng - Seri Informatika* 3(1): 34.

[17] Wongkar, Steven, Alicia Sinsuw, and Xaverius Najoan. 2015. “Analisa Implementasi Jaringan InternetDengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II.” *E-journal Teknik Elektro dan Komputer* 4(6): 62–68.