Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Mikrotik-based Firewall as a Filter Site Blocking in Pahunga Lodu Secretariat

Meyfrita Hada Indah Nggandung[1*], Fajar Hariadi[2], Novem Berlian Uly[3]

[1,2,3]*Program Studi Teknik Informatika, Universitas Kristen Wira Wacana Sumba*
meyfritahada@gmail.com [1*], fajar@unkriswina.ac.id [2], novemuly@unkriswina.ac.id [3]

Abstract

The rapid development of information technology has had a significant impact on various aspects of life, including the government agency environment. One of the challenges faced is the misuse of internet access by employees, which can reduce work productivity, such as accessing online gambling sites and adult content. This study was conducted at the Pahunga Lodu Subdistrict Secretariat with the aim of analyzing the effectiveness of implementing a MikroTik-based firewall in blocking access to websites irrelevant to work activities. The method used involved configuring the firewall on the MikroTik RouterOS device with features such as Web Filtering, DNS Filtering, and Layer 7 Protocol. Data collection was conducted through direct observation of network activity before and after the implementation of the firewall, as well as interviews with employees regarding its impact on work productivity. Additionally, testing was performed using Quality of Service (QoS) parameters such as throughput, packet loss, delay, and jitter to assess network performance after the system implementation. The results of the study indicate that the MikroTik firewall is effective in blocking access to unwanted websites and helps maintain stability and efficiency in bandwidth usage. Based on interviews, the majority of employees support the implementation of this system because it has a positive impact on the work environment. This study contributes to improving network security and work efficiency in the government environment and can serve as a reference for the implementation of similar technologies in other institutions. The implementation of web filtering also has a positive impact on overall network quality. A 10-minute test showed an improvement in Quality of Service (QoS) parameters, with throughput increasing from 335.60 kbps to 380.16 kbps (+44.56 kbps), packet loss decreasing from 2.76% to 1.64% (−1.12%), delay decreased from 13.7 ms to 12.2 ms (−1.5 ms), and jitter decreased from 16.93 ms to 12.15 ms (−4.78 ms).

Keywords: *Firewall, MikroTik, Web Filtering, Network Security, Government, QoS*

1. Introduction

The rapid development of information and communication technology has had a significant impact on various aspects of life, including the world of work and government[1]. In this digital age, the Internet has become one of the primary tools supporting administrative activities and public services in government offices, including the Pahunga Lodu Subdistrict Secretariat. However, uncontrolled Internet use can lead to misuse of access, such as accessing online gambling sites and adult websites while working, thereby reducing employee productivity.

One solution that can be implemented to address this issue is to apply a MikroTik-based firewall as a website blocking filter. MikroTik is a network device with advanced firewall features, enabling network administrators to restrict access to specific websites. With proper configuration, this system can help control internet usage in the workplace.

Therefore, this study aims to implement a MikroTik-based firewall configuration to filter and block access to online gambling sites and pornographic content in government tasks at the Pahunga Lodu Secretariat. The implementation of this system is expected to increase work productivity and ensure more optimal use of the internet in supporting services to the community.

2. Research Method

The method used was firewall configuration on MikroTik RouterOS devices with Web Filtering, DNS Filtering, and Layer 7 Protocol features[2]. Data collection was carried out through direct observation of network activity before and after firewall implementation, as well as interviews with employees regarding its impact on work productivity[3]. Additionally, testing was conducted using Quality of Service (QoS) parameters such as throughput, packet loss, delay, and jitter to assess network performance after the system implementation[4].

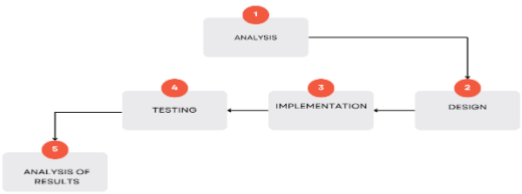


Fig. 1: Research process

2.1 Analysis

The observation was conducted by visiting the Pahunga Lodu Subdistrict Secretariat Office to access websites containing pornography and online gambling before the implementation of web filtering on the firewall. In addition, the author also interviewed one of the operators at the office to obtain information relevant to the research. The results of the interviews conducted by the researcher at the Pahunga Lodu Subdistrict Secretariat with the office operator are as follows:

The internet network at the Pahunga Lodu Secretariat has been used for activities related to office tasks such as sending and receiving data within the village, between subdistricts, and to the district and even the province. Furthermore, the internet network is also used for webinars or online meetings via Zoom, and all employees use the internet to access important information and personnel application services. The internet network at the Pahunga Lodu Subdistrict Secretariat is known to have a bandwidth of 2 Mbps.

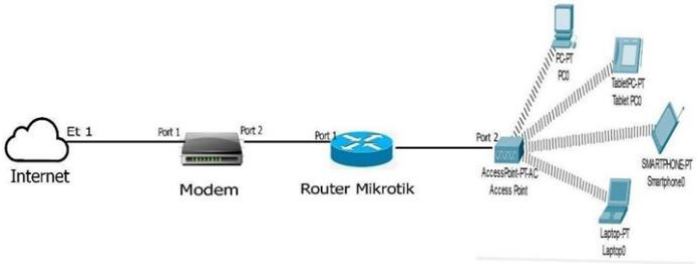


Fig. 2: Network Topology Before Implementing Web Filtering Firewall

From the data obtained from interviews and observations, it was found that the current topology at the Pahunga Lodu Secretariat is as shown in the figure above, which has one access point. The Pahunga Lodu Subdistrict Secretariat uses BAKTI KOMINFO as its internet service provider (ISP) with a bandwidth of 2 Mbps. The network topology at the Pahunga Lodu Secretariat consists of a series of connections starting from the internet service provider connected to a modem using port 1, then from the modem it is forwarded to a Mikrotik router using port 1, but within this Mikrotik router, firewall filtering has not yet been implemented.

The tests conducted prior to implementing firewall filtering on the websites to be blocked are as follows:

Table 1: Test Table

No	Site Name	Site Type	Website Status
1.	https://www.xnxx.com/	Pornography	Accessible
2.	https://www.pornhub.com/	Pornography	Accessible
3.	https://www.redtube.com/	Pornography	Accessible
4.	https://www.xvideos.com/	Pornography	Accessible
5.	https://www.youporn.com/	Pornography	Accessible
6.	https://www.spankbang.com/	Pornography	Accessible
7.	https://www.888casino.com/	Online Gambling	Accessible
8.	https://www.pokerstars.com/	Online Gambling	Accessible
9.	https://www.williamhill.com/	Online Gambling	Accessible
10.	https://www.betway.com/	Online Gambling	Accessible
11.	https://www.1xbet.com/	Online Gambling	Accessible
12.	https://www.unibet.com/	Online Gambling	Accessible
13.	https://www.leovegas.com/	Online Gambling	Accessible

14	https://www.bovada.com/	Online Gambling	Accessible
15	https://www.draftkings.com/	Online Gambling	Accessible
16	https://www.fanduel.com/	Online Gambling	Accessible
17	https://www.betfair.com/	Online Gambling	Accessible
18	https://www.paddypower.com/	Online Gambling	Accessible
19	https://www.ladbrokes.com/	Online Gambling	Accessible
20	https://www.bet365.com/	Online Gambling	Accessible
21	https://www.pinnacle.com/	Online Gambling	Accessible
22	https://www.betfred.com/	Online Gambling	Accessible
23	https://www.royalpanda.com/	Online Gambling	Accessible
24	https://www.comeon.com/	Online Gambling	Accessible
25	https://www.betsson.com/	Online Gambling	Accessible

Based on initial testing conducted on adult content and online gambling sites, these sites can still be accessed smoothly using the office Wi-Fi, so it can be proven that the internet network is not yet protected because there is no protection in the form of technology[5].
After conducting initial testing, researchers measured network quality using Wireshark to obtain QOS tests such as throughput, packet loss, delay, and jitter as follows
After conducting initial testing, the researchers measured network quality using Wireshark to obtain QOS testing such as throughput, packet loss, delay, and jitter as follows[6].

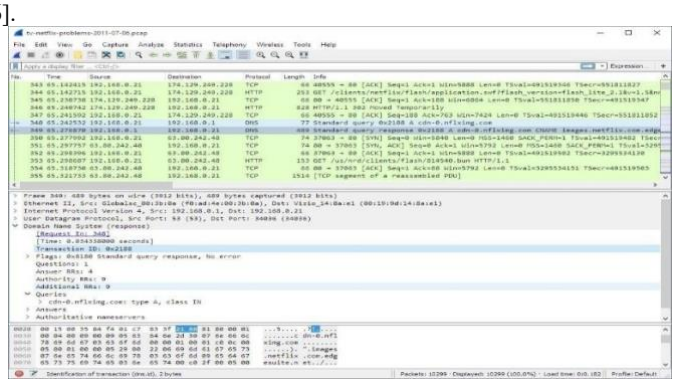


Fig. 3: Wireshark Screen Capture

Based on the results captured during a 10-minute period, the following QOS tests were conducted: throughput, packet loss, delay, and jitter.

a. *Throughput* : *!tcp.analysis.flags &&tcp*

$$\frac{number\ of\ bytes}{Time\ Span} = \frac{25{,}180{,}132}{600.147} = 41{,}950.88 \text{ byte} \times 8$$
$$= 335{,}600.96 \text{ kbps}$$

b. *Packet Loss* : !tcp.analysis.lost_segment

$$\frac{lost\ packets}{total\ packets} \times 100\% = \frac{1.210}{43{,}800} \times 100\%$$
$$= 2.7623\ \%$$

c. *Delay* : !tcp.analysis.flags

$$Delay = \frac{Total\ Delay}{received\ package} = \frac{600.147}{43{,}800}$$

$$average\ delay = 0.0137 \times 1000 \text{ second}$$
$$= 13.7 \text{ mili second}$$

d. *Jitter*

$$Jitter = \frac{total\ delay\ variation}{(Total\ packets - 1)} = \frac{720.90 \text{ second}}{(42{,}589)}$$
$$= 0.01693\ second$$
$$= 16.93 \text{ mili second}$$

The following is a table of QoS results and categories in Table 2

The following is the Table of Estimation *of QoS* results and their categories in table 2

No.	QoS Parameters	Calculation Results	Category	Index
a.	*Throughput*	335.60 kbps	Very Good	4
b.	*Packet Loss*	2.76%	Good	3
c.	*Delay*	13.7 ms	Very Good	4
d.	*Jitter*	16.93 ms	Good	3

2.2 System Design

Here is the topology created to be applied to the Pahunga Lodu Secretariat.

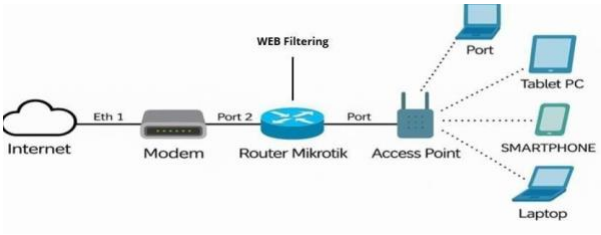


Fig. 4: Network Topology After *Web Filtering Implementation Firewall*

The design of the network topology in the image above is a design that aims to implement a *web filtering firewall* system by configuring the *Mikrotik router, in order to filter and block access to negative sites that can interfere with the focus or mental health of network users at the Pahunga Lodu Secretariat*[7].

In the design of this network topology, no changes were made to the main network structure that already existed at the Pahunga Lodu Secretariat. However, there is an addition of *a web filtering firewall* feature to the Mikrotik device used, so that every device connected to *wifi* in the secretariat environment can be automatically protected from negative content and online gambling sites[8].

2.3 Implementation

The *web filtering* configuration that is applied refers to a predefined list of specific sites or categories, so that the system can perform filtering effectively and efficiently, following a list of filtered content.

Table 3: List of Filtered Content

No.	Name	Filters Used
1.	Sites	(\.|^)xnxx\.com$ (\.|^)pornhub\.com$ (\.|^)redtube\.com$ (\.|^)xvideos\.com$ (\.|^)youporn\.com$ (\.|^)spankbang\.com$
2.	Online Gambling Sites	(\.|^)bet365\.com$ (\.|^)888casino\.com$ (\.|^)pokerstars\.com$ (\.|^)williamhill\.com$ (\.|^)betway\.com$ (\.|^)1xbet\.com$ (\.|^)unibet\.com$ (\.|^)leovegas\.com$ (\.|^)bovada\.com$ (\.|^)draftkings\.com$ (\.|^)fanduel\.com$ (\.|^)betfair\.com$ (\.|^)paddypower\.com$ (\.|^)ladbrokes\.com$ (\.|^)bet365\.com$ (\.|^)pinnacle\.com$ (\.|^)betfred\.com$ (\.|^)royalpanda\.com$ (\.|^)comeon\.com$ (\.|^)betsson\.com$

In an effort to limit access to negative content such as gambling and pornography sites, an effective technical method is regular expression-based *blocking (RegEx).* This technique is generally applied to systems such as Mikrotik routers, *DNS filtering tools*, or *web proxies.*

A regular expression is a text-matching pattern used to recognize specific domains or URLs that are set as prohibited. Using *RegEx,* the system can automatically filter and block access requests to sites that contain certain elements, such as domain names related to gambling and pornography.

2.4 Testing

The test in this study aims to evaluate the effectiveness of the application of *web filtering firewall* on the quality of network service (*QoS*) in the Pahunga Lodu District Secretariat. The evaluation was carried out by comparing the test results before and after *the firewall* was applied over a period of 10 minutes. The *analyzed QoS* parameters include *throughput*, packet *loss*, *delay*, and *jitter*, which are calculated based on the standard technical formula of network measurement.

Testing is carried out systematically to obtain accurate and relevant data on network conditions. Through the calculation of the value of each parameter, it can be seen that there are significant changes after the *firewall* is applied. The results of this comparison are presented in the form of a table to make it easier for readers to understand the direction of change, both in the form of improving and decreasing network performance. This table serves as a basis for drawing conclusions about the extent to which *firewalls* contribute to improving the efficiency and stability of internet networks in government agencies.

Table 4 Test Table

Testing	Before Testing	After Testing
Throughput	265.32 kbps	380.16 kbps
Packet Loss	4.85 %	1.636%
Delay(Latency)	21.2ms	12,2ms
Jitter	27.8 ms	12.15 ms

2.5 Analysis of Results

In the final result analysis section, a comparison was made between the test results before and after the implementation *of the web filtering firewall* at the Pahunga Lodu Secretariat. This analysis focused on measuring Quality *of Service (QoS)* values during the 10-minute test duration, using relevant formulas, such as *throughput*, *delay*, *packet loss*, and *jitter*. Observations were made to see the extent to which there was an increase or decrease in *QoS* value after *the firewall* was implemented, particularly in restricting access to online gambling and pornography sites. The results of this measurement will provide an overview of the effectiveness of the implementation of *the filtering* system on the quality of internet network services used.

In the calculation of the analysis of changes *in Quality of Service (QoS)* before and after the implementation *of web filtering firewall* at the Pahunga Lodu Secretariat, a formula for changes in *the value of QoS* parameters was used to measure the percentage increase or decrease rate. The change formula used is:

Table 5 QoS percentage

Parameter	Percentage Decrease/Increase
Throughput	26,52%
Packet Loss	43,09%
Delay	35,38%
Jitter	39,12%

3. Result and Discussion

This chapter will describe the results of implementing a web filtering system on the network of the Pahunga Lodu Subdistrict Secretariat[9]. The main focus of the developed system is to restrict access to websites that are considered inappropriate in the workplace, particularly those containing gambling and pornographic content. This implementation was carried out as a form of strengthening the policy of healthy and responsible internet use in government agencies.

This chapter will explain in detail how the web filtering system was implemented, including the network architecture, content-based blocking mechanisms, and the configuration used on the MikroTik router device. Subsequently, testing was conducted on the implemented system to evaluate two main aspects: the effectiveness of content filtering and its impact on network service quality (Quality of Service/QoS). The testing was conducted using a scenario where access to prohibited sites was attempted from various devices to ensure that the system could consistently recognize and block requests to gambling and pornography sites.

The testing was conducted under real-world conditions involving a number of respondents[10] who are active users of the network within the Secretariat. User feedback was also collected to assess the extent to which the system affects the comfort and ease of accessing internet services. This aims to obtain a comprehensive evaluation of the system implementation, both from a technical perspective and user experience. The test results are expected to provide an objective overview of the effectiveness of the web filtering system in creating a safer and more productive digital work environment, while ensuring that access restriction policies do not compromise network connectivity quality.

3.1 Accessing Mikrotik Using Winbox

The initial process of implementing the system begins by connecting the MikroTik device using the official Winbox application[11] to configure the network. In this implementation, a MikroTik RB951G-2HnD router is used, which is accessed through the Winbox home screen after the device is detected. Before configuration is performed, the router is first ensured to be connected to the internet source from the ISP via an Ethernet cable plugged into port 1 (ether1), which functions as the WAN port. This connection originates from the ISP's modem or access point, which has been previously connected via a PoE cable or directly from the Ethernet port. This step is important to ensure the device has internet access so that further configuration processes, such as IP settings, NAT, DNS, and the implementation of web filtering features, can proceed smoothly.

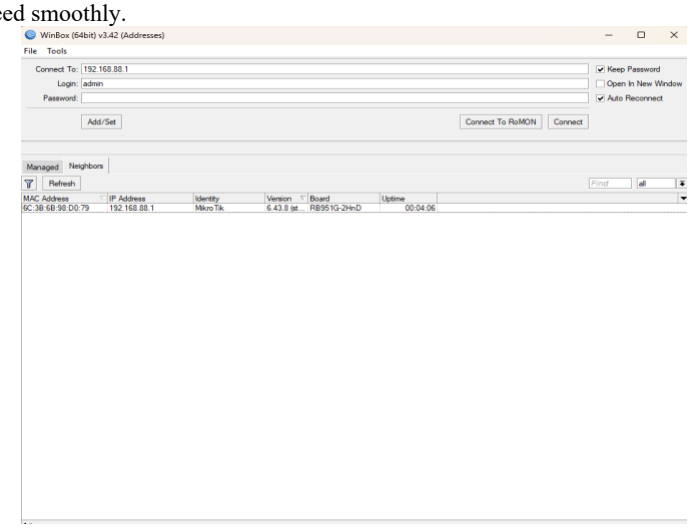


Fig. 5: Accessing Mikrotik Using Winbox

3.2 Accessing the Mikrotik Network and Main Menu

After selecting the connected network via the Neighbors menu at the bottom of the Winbox application, the next step is to fill in the login field with the username and password corresponding to the settings on the MikroTik router, which is intended to maintain the security of the data and configurations stored on the device. However, in the initial configuration, the default account with the username “admin” and a blank password is usually used. After successfully logging in, users will be directed to the main MikroTik interface, which serves as the central hub for managing various network configurations such as IP settings, firewall, NAT, DNS, and other advanced features required for system implementation.

Fig. 6: Mikrotik Main Menu

3.2 Accessing the Interface Menu

The next step is to access the Interface menu on MikroTik to ensure that the internet connection is properly connected through the port being used, where in this implementation Ethernet port 1 (ether1) functions as the WAN port that receives the internet source from the WiFi device connected to the ISP. Although at the initial stage of using the MikroTik device, it is not yet possible to directly access the internet, the device can still be configured through Winbox. To enable all devices connected to the router to access the internet, configuration is required so that each port used can obtain an IP address and be directed to use the internet connection originating from the ether1 port.

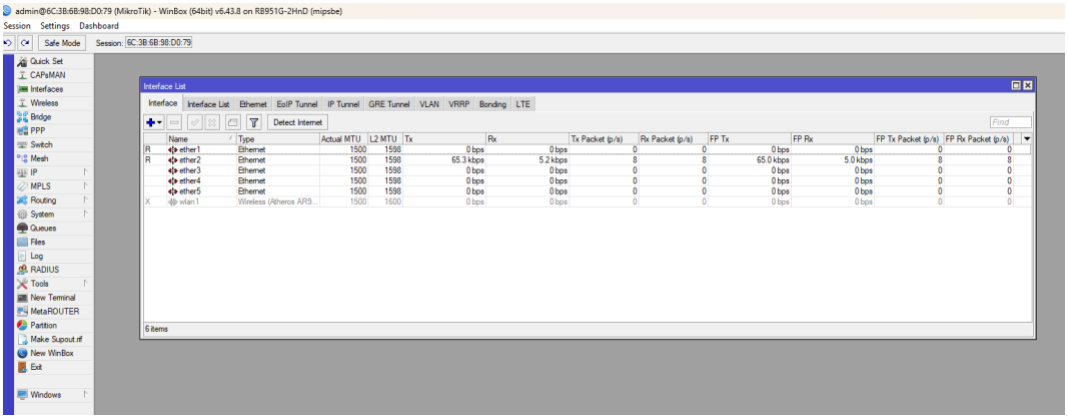


Fig. 7: The Interface Menu

3.3 Labeling Interfaces

To simplify the configuration process and minimize the risk of errors in network settings, each port that will be used can be labeled (named) according to its respective function. In this implementation, labeling is optional; however, for this instance, labeling is performed as follows: Ethernet port 1, which serves as the receiver for the internet connection from the ISP via the WiFi device, is labeled ether1_isp, while Ethernet port 2, which is directly connected to the laptop for configuration purposes, is labeled ether2_laptop. With this labeling, the identification of each port becomes clearer, making it easier to perform further configuration processes such as setting IP addresses, NAT, and creating firewall rules according to system requirements.

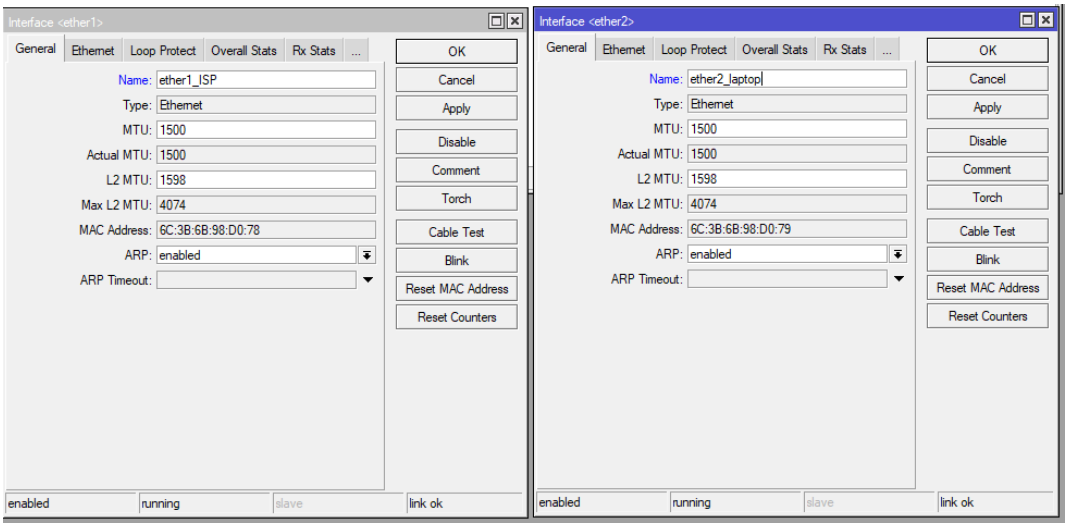


Fig. 8: Labeling Interfaces

3.4 DHCP Client Check

The next step is to check whether the ether1_isp port has successfully obtained an IP address from the WiFi network connected to the ISP. This check can be done through the New Terminal menu in Winbox by typing the command /ip dhcp-client print. This command will display the status of the active DHCP client on the router, including information on whether the ether1_isp port has obtained an IP address automatically. This step is important to ensure that the router is successfully connected to the internet source before proceeding to the internal network configuration process and IP distribution to other ports.

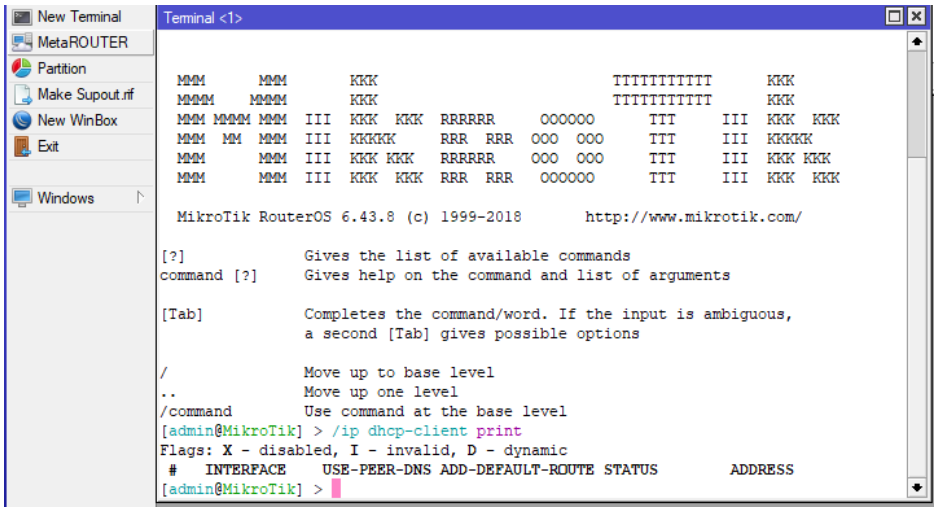


Fig. 9: DHCP Client Check

Based on the results of the /ip dhcp-client print command, it is known that the ether1_isp port and other ports have not obtained an IP address from the previously connected WiFi network source. This indicates that the MikroTik router has not successfully connected to the internet, even though obtaining an IP address from the DHCP server is a prerequisite for the router to access the internet. Therefore, additional configuration is required on the DHCP client to ensure that the ether1_isp port can automatically receive an IP address from the ISP network as the first step before internal network configuration and other features can be implemented.

3.5 Assigning IP DHCP Client on Ethernet 1

After confirming that the ether1_isp port has not been assigned an IP address, the next step is to add a DHCP client to that port so that the router can automatically receive an IP address from the WiFi network connected to the ISP. This configuration is performed via the terminal using the command /ip dhcp-client add interface=ether1_isp use-peer-dns=yes add-default-route=yes disabled=no. This command enables the DHCP client on the ether1_isp interface, allows the use of DNS from the ISP, and adds a default route so that the router can connect to the internet. After the configuration is added, a verification can be performed using the command /ip dhcp-client print. If successful, information will appear indicating that the ether1_isp interface has obtained an IP address with a "bound" status, signifying that the connection to the ISP network is established and the router is ready for further configuration.

```
[admin@MikroTik] > /ip dhcp-client add interface=ether1 use-peer-dns=yes add-defau
lt-route=yes disabled=no
[admin@MikroTik] > /ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
 #   INTERFACE    USE-PEER-DNS ADD-DEFAULT-ROUTE STATUS        ADDRESS
 0   ether1_ISP   yes          yes               bound         192.168.8.101/24
[admin@MikroTik] >
```

Fig. 10: DHCP Client Check

Based on the results of the check after adding the DHCP client, it was found that the ether1_isp interface successfully obtained the IP address 192.168.8.101/24 from the DHCP server originating from the ISP WiFi network. This indicates that the DHCP client configuration is working properly, as indicated by the bound status in the previous command results. As a result, the MikroTik router is now connected to the internet via the ether1_isp interface, which serves as a crucial foundation for continuing internal network configuration and implementing features such as NAT, DNS, and web filtering.

3.6 Assignment of NAT and SET DNS Servers

To provide internet access to devices on the local network via a MikroTik router, NAT (Network Address Translation) configuration using the masquerade method is required. This configuration works by masking the local IP addresses of client devices with the public IP address owned by the interface connected to the internet, namely ether1_isp. This process allows multiple local devices to use a single public IP address simultaneously when accessing the internet. This NAT is configured via the terminal using the command /ip firewall nat add chain=srcnat out-interface=ether1_isp action=masquerade. This command instructs MikroTik to masquerade all outgoing traffic through the ether1_isp interface, so that the ISP device can recognize and respond to the data packets sent, and MikroTik will forward them back to the appropriate client device. This configuration is crucial for ensuring smooth and efficient communication between the local network and the internet.

```
[admin@MikroTik] > /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
[admin@MikroTik] > /ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
[admin@MikroTik] > ip dns print
                    servers: 8.8.8.8,1.1.1.1
           dynamic-servers: 192.168.8.1
      allow-remote-requests: yes
        max-udp-packet-size: 4096
       query-server-timeout: 2s
        query-total-timeout: 10s
    max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
                 cache-size: 2048KiB
             cache-max-ttl: 1w
                cache-used: 18KiB
```

Fig. 11: Assignment of NAT and SET DNS Servers

3.7 Configuration Check

After performing a series of configurations, starting from adding a DHCP client to the ether1_isp interface, configuring NAT using the masquerade method, to setting up DNS IP, the next step is to perform a check to ensure that all configurations are functioning properly. This verification is performed using several commands in the MikroTik terminal. First, the command /ip dhcp-client print is used to display the status of the DHCP client and ensure that the ether1_isp interface has successfully obtained an IP address from the modem or ISP. Second, the command /ip route print displays the routing table, which is useful for ensuring the presence of a default route with the destination 0.0.0.0/0 as the primary path to the internet. Next, the /ip firewall nat print command is used to check whether NAT rules have been added, particularly the masquerade rule, which masks the local network IP address as the public IP address of the ether1_isp interface so that client devices can access the internet. Finally, the /ip dns print command is used to display the active DNS configuration, including the DNS server addresses being used and the status of DNS requests from clients. By running these four commands, the administrator can ensure that the router is ready to connect the local network to the internet with the correct and stable configuration.

```
[admin@MikroTik] > /ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
 #   INTERFACE                  USE-PEER-DNS ADD-DEFAULT-ROUTE STATUS       ADDRESS
 0   ether1_ISP                 yes          yes               bound        192.168.8.101/24
[admin@MikroTik] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADS  0.0.0.0/0                          192.168.8.1               1
 1 ADC  192.168.8.0/24     192.168.8.101   ether1_ISP                0
[admin@MikroTik] > /ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade out-interface=ether1_ISP
[admin@MikroTik] > /ip dns print
                    servers: 8.8.8.8,1.1.1.1
          dynamic-servers: 192.168.8.1
       allow-remote-requests: yes
         max-udp-packet-size: 4096
        query-server-timeout: 2s
         query-total-timeout: 10s
     max-concurrent-queries: 100
max-concurrent-tcp-sessions: 20
                cache-size: 2048KiB
            cache-max-ttl: 1w
               cache-used: 18KiB
```

Fig. 12: Assignment of NAT and DNS Servers

3.8 Creating a Bridge, IP POOL, and DHCP Server

After the ether1_isp interface successfully obtains an IP address and connects to the internet, the next step is to configure the remaining interfaces, namely ether2 to ether5, as well as wlan1 (MikroTik wireless), so that the entire local network can connect to the internet efficiently. Rather than manually configuring IP addresses for each interface, a more practical and centralized configuration is achieved by creating a bridge that combines all these interfaces. The interfaces combined into this bridge are ether2–ether5 and wlan1, so that all devices connected via LAN cable or WiFi will be on the same local network. After the bridge is added and wlan1 is activated in AP-Bridge mode (Access Point Bridge), the MikroTik router will usually perform a brief restart. Upon re-entering Winbox, the Interfaces menu will show that wlan1 is active and the bridge-LAN interface has been formed, containing the combined ether2–ether5 and wlan1 interfaces. This configuration not only simplifies network management but also facilitates web filtering and QoS settings since all local clients are on a single integrated network path.

/interface bridge add name=bridge-LAN
/interface bridge port add bridge=bridge-LAN interface=ether2
/interface bridge port add bridge=bridge-LAN interface=ether3
/interface bridge port add bridge=bridge-LAN interface=ether4
/interface bridge port add bridge=bridge-LAN interface=ether5
/interface wireless set wlan1 disabled=no mode=ap-bridge ssid="WiFi_Pahunga Lodu" frequency=2412 band=2ghz-b/g/n
/interface bridge port add bridge=bridge-LAN interface=wlan1
/interface bridge port print

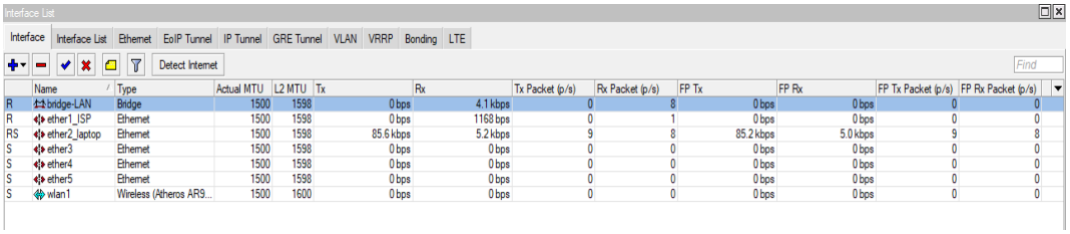


Fig. 13: Bridge-LAN Creation

The configuration at this stage aims to integrate all local network interfaces, both wired and wireless, into a single unified network using the bridge feature on MikroTik. First, a bridge named bridge-LAN is created to serve as the connection between local interfaces. Then, the physical interfaces from ether2 to ether5 are added to the bridge so that all devices connected through those ports are integrated into the same network. Next, the wireless interface wlan1 is enabled and configured in ap-bridge mode, and given the SSID “WiFi_Pahunga Lodu” using the 2412 MHz frequency (channel 1) with 2GHz b/g/n band support. The wlan1 interface is also added to the bridge-LAN, so that

the WiFi connection will be on the same network as the wired connection. To ensure that all interfaces have successfully joined the bridge, the command /interface bridge port print is used. With this configuration, all devices connected via cable on ports ether2–ether5 and via WiFi wlan1 will be in the same network segment and can easily connect to each other.

```
[admin@MikroTik] > /ip dhcp-server print
Flags: D - dynamic, X - disabled, I - invalid
 #    NAME                INTERFACE                RELAY          ADDRESS-POOL                LEASE-TIME ADD-ARP
[admin@MikroTik] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 192.168.8.101/24   192.168.8.0     ether1_ISP
[admin@MikroTik] > /ip address add address=192.168.10.1/24 interface=bridge-LAN
[admin@MikroTik] > /ip pool add name=pool-LAN ranges=192.168.10.10-192.168.10.100
[admin@MikroTik] > /ip dhcp-server add name=dhcp-LAN interface=bridge-LAN address-pool=pool-LAN disabled=no
[admin@MikroTik] > /ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-server=8.8.8.8,1.1.1.1
[admin@MikroTik] >
```

Fig. 14: Creating an IP POOL and DHCP Server on a Bridge

/ip dhcp-server print This command is used to check whether there is an active DHCP server. The result is empty (only the title column and "flags"), indicating that no DHCP service has been configured previously.

/ip address print Displays all IP addresses assigned to the router. One address, 192.168.8.101/24 (flagged D = dynamic), is assigned to ether1_ISP, confirming that the WAN interface has obtained an IP address from the DHCP modem/ISP.

/ip address add address=192.168.10.1/24 interface=bridge-LAN Adds the IP address 192.168.10.1/24 to the bridge-LAN interface (combination of ether2-ether5 + wlan1). This address will serve as the gateway for all LAN devices.

/ip pool add name=pool-LAN ranges=192.168.10.10-192.168.10.100 Creates an IP address pool to be leased by DHCP to clients, namely 192.168.10.10–192.168.10.100.

/ip dhcp-server add name=dhcp-LAN interface=bridge-LAN address-pool=pool-LAN disabled=no Set up a DHCP server named dhcp-LAN on the bridge-LAN interface, using the newly created pool, and enable it immediately (disabled=no).

/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-server=8.8.8.8,1.1.1.1 Defining DHCP network parameters: subnet 192.168.10.0/24, gateway 192.168.10.1 (router address), and public DNS from Google (8.8.8.8) and Cloudflare (1.1.1.1).

With the above commands, the router now provides DHCP services for the LAN: clients connected to ether2-ether5 or Wi-Fi (wlan1) will automatically receive an IP address in the range 192.168.10.10-100, with a gateway of 192.168.10.1, and DNS servers 8.8.8.8 and 1.1.1.1, enabling them to directly access the internet via the previously configured NAT on ether1_ISP.

3.9 Implementation of Web Filtering

To add a domain address to be filtered using the Layer7 Protocol method on MikroTik, you can use the terminal command (CLI) with the following basic syntax: /ip firewall layer7-protocol add name=filter_name regexp="^.* (domain_to_be_blocked).*". This command creates a pattern (regular expression) that MikroTik will recognize as an indicator of traffic heading to the domain you want to block. For example, if you want to block the pornhub.com site, the command would be: /ip firewall layer7-protocol add name=block-pornhub regexp="^.*(pornhub\\.com).*". The \\. symbol is used to prevent the period from being interpreted as a wildcard in the regular expression, and .* is used to match any characters before or after the domain.

```
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-redtube regexp="^.*(redtube\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-xvideos regexp="^.*(xvideos\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-youporn regexp="^.*(youporn\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-spankbang regexp="^.*(spankbang\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-bet365 regexp="^.*(bet365\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-888casino regexp="^.*(888casino\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-pokerstars regexp="^.*(pokerstars\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-williamhill regexp="^.*(williamhill\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-betway regexp="^.*(betway\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-1xbet regexp="^.*(1xbet\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-unibet regexp="^.*(unibet\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-leovegas regexp="^.*(leovegas\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-bovada regexp="^.*(bovada\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-draftkings regexp="^.*(draftkings\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-fanduel regexp="^.*(fanduel\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-betfair regexp="^.*(betfair\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-paddypower regexp="^.*(paddypower\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-ladbrokes regexp="^.*(ladbrokes\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-pinnacle regexp="^.*(pinnacle\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-betfred regexp="^.*(betfred\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-royalpanda regexp="^.*(royalpanda\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-comeon regexp="^.*(comeon\\.com).*"
[admin@MikroTik] > /ip firewall layer7-protocol add name=blok-betsson regexp="^.*(betsson\\.com).*"
```

Fig. 15: Adding Addresses to be Filtered

After successfully adding the address to be filtered, next ensure that the address entered is actually registered so that a rule can be added to the existing list.

```
[admin@MikroTik] > /ip firewall layer7-protocol print
 # NAME                                                                    REGEXP
 0 blok-pornhub                                                            ^.*(pornhub\.com).*
 1 blok-xnxx                                                               ^.*(xnxx\.com).*
 2 blok-redtube                                                            ^.*(redtube\.com).*
 3 blok-xvideos                                                            ^.*(xvideos\.com).*
 4 blok-youporn                                                            ^.*(youporn\.com).*
 5 blok-spankbang                                                          ^.*(spankbang\.com).*
 6 blok-bet365                                                             ^.*(bet365\.com).*
 7 blok-888casino                                                          ^.*(888casino\.com).*
 8 blok-pokerstars                                                         ^.*(pokerstars\.com).*
 9 blok-williamhill                                                        ^.*(williamhill\.com).*
10 blok-betway                                                             ^.*(betway\.com).*
11 blok-lxbet                                                              ^.*(lxbet\.com).*
12 blok-unibet                                                             ^.*(unibet\.com).*
13 blok-leovegas                                                           ^.*(leovegas\.com).*
14 blok-bovada                                                             ^.*(bovada\.com).*
15 blok-draftkings                                                         ^.*(draftkings\.com).*
16 blok-fanduel                                                            ^.*(fanduel\.com).*
17 blok-betfair                                                            ^.*(betfair\.com).*
18 blok-paddypower                                                         ^.*(paddypower\.com).*
19 blok-ladbrokes                                                          ^.*(ladbrokes\.com).*
20 blok-pinnacle                                                           ^.*(pinnacle\.com).*
21 blok-betfred                                                            ^.*(betfred\.com).*
22 blok-royalpanda                                                         ^.*(royalpanda\.com).*
23 blok-comeon                                                             ^.*(comeon\.com).*
```

Fig. 16: Checking addresses to be filtered

After adding the Layer7 protocol, the next step is to add a rule in the firewall filter with a command such as /ip firewall filter add chain=forward action=drop layer7-protocol=blok-pornhub comment="Block pornhub", which serves to actively block traffic that matches the pattern.

```
[admin@MikroTik] > /ip firewall filter
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-xnxx action=drop comment="Blokir xnxx"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-pornhub action=drop comment="Blokir pornhub"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-redtube action=drop comment="Blokir redtube"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-xvideos action=drop comment="Blokir xvideos"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-youporn action=drop comment="Blokir youporn"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-spankbang action=drop comment="Blokir spankban
g"
[admin@MikroTik] /ip firewall filter>
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-bet365 action=drop comment="Blokir bet365"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-888casino action=drop comment="Blokir 888casin
o"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-pokerstars action=drop comment="Blokir pokerst
ars"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-williamhill action=drop comment="Blokir willia
mhill"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-betway action=drop comment="Blokir betway"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-lxbet action=drop comment="Blokir lxbet"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-unibet action=drop comment="Blokir unibet"
[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-leovegas action=drop comment="Blokir leovegas"

[admin@MikroTik] /ip firewall filter> add chain=forward layer7-protocol=blok-bovada action=drop comment="Blokir bovada"
```

Fig. 17: Filtering Implementation

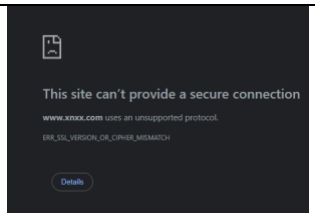
Next, do the same thing to check whether the list has been entered into the rule used to block previously registered sites.

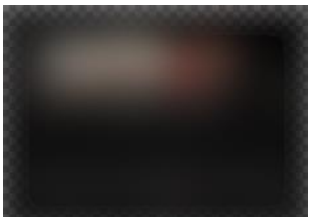
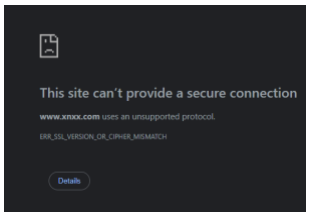
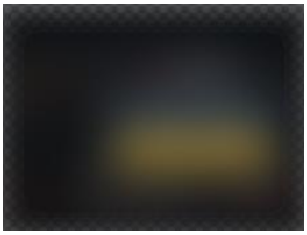
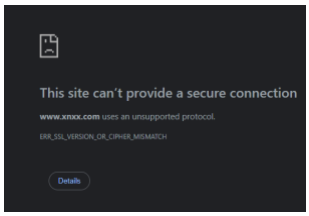
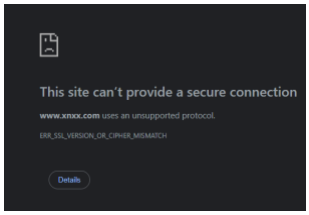
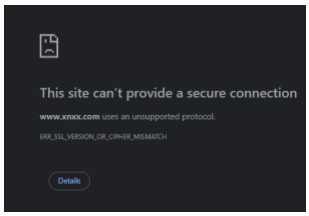
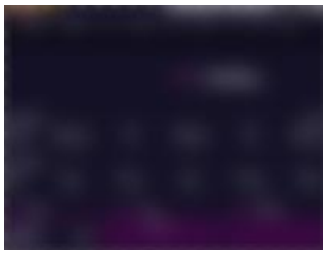
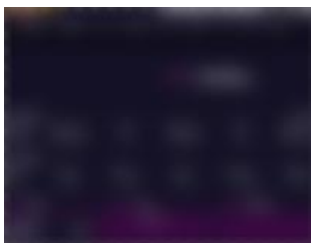
```
[admin@MikroTik] /ip firewall filter> /ip firewall filter print where action=drop
Flags: X - disabled, I - invalid, D - dynamic
 0    ;;; Blokir xnxx
      chain=forward action=drop layer7-protocol=blok-xnxx

 1    ;;; Blokir pornhub
      chain=forward action=drop layer7-protocol=blok-pornhub

 2    ;;; Blokir redtube
      chain=forward action=drop layer7-protocol=blok-redtube

 3    ;;; Blokir xvideos
      chain=forward action=drop layer7-protocol=blok-xvideos

 4    ;;; Blokir youporn
      chain=forward action=drop layer7-protocol=blok-youporn

 5    ;;; Blokir spankbang
      chain=forward action=drop layer7-protocol=blok-spankbang
```

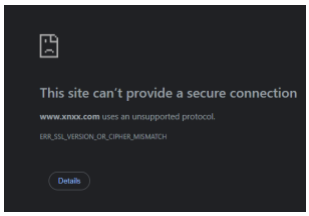
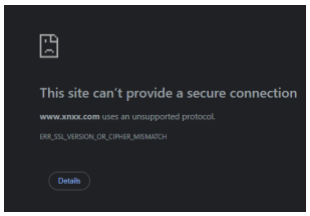
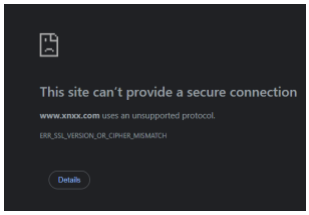
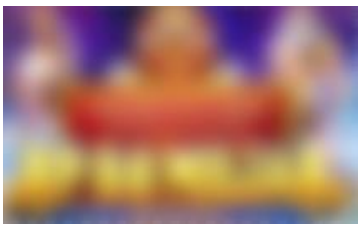
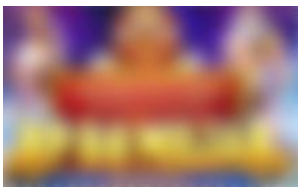
Fig. 18: Checking the Filtering List and drop action

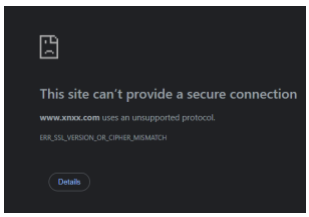
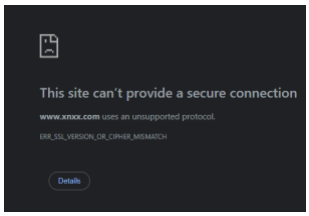
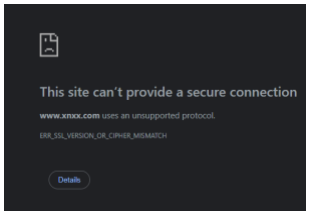
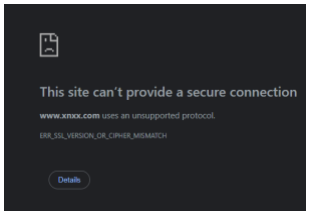
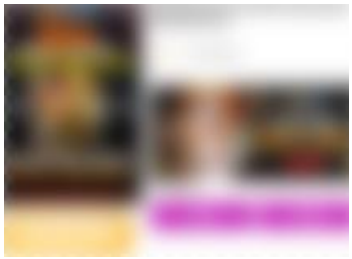
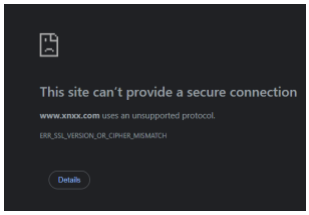
3.10 Web Filtering Results

Table 6

Site Name	Before Implementation	After Implementation
https://www.xnxx.com/		

https://www.pornhub.com/		
https://www.redtube.com/		
http://www.xvideos.com/		
http://www.youporn.com/		
https://www.spankbang.com/		
https://www.888casino.com/		
https://www.pokerstars.com/		
https://www.williamhill.com/		

http://www.betway.com/		
http://www.1xbet.com/		
http://www.unibet.com/		
https://www.leovegas.com/		
http://www.bovada.com/		
http://www.draftkings.com/		
https://www.fanduel.com/		
http://www.betfair.com/		

https://www.paddypower.com/		
http://www.pinnacle.com/		
https://www.betfred.com/		
https://www.royalpanda.com/		
https://www.comeon.com/		
https://www.betsson.com/		

Websites that have been successfully blocked using the Layer7 Protocol method on MikroTik devices show effective results, where when tested through various access methods, including using incognito mode on browsers, these websites remain inaccessible. This indicates that the blocking is done at the network layer, not just at the browser or user device level. In other words, even if users attempt to bypass the blocking using incognito mode, browser VPNs, or clearing the cache, access to the websites is still denied because the firewall rules directly filter data traffic that matches the predefined patterns. This result demonstrates that while Layer7 methods have limitations in handling HTTPS-based websites, in certain cases and for specific types of websites—particularly those that have not fully encrypted their traffic or have not implemented complex CDNs—this method remains capable of achieving effective blocking, as evidenced by consistent connection failures on both regular browsers and incognito tabs. This also indicates that the implemented firewall system has strong control over internet access policies within the local network.

Some websites remain accessible even though they are listed in the firewall rules. This occurs because most modern websites, including online gambling and pornography sites, use the HTTPS protocol, which encrypts the content of communication between the client and server. Since Layer7 methods work by scanning text patterns (regular expressions) in data traffic payloads, when data is encrypted (as in HTTPS), and since most internet traffic is now protected by SSL/TLS encryption, firewalls cannot directly identify the applications or services being used based solely on network packet metadata. This makes Layer7-based rules less effective, as application protocol identification is difficult without sufficient information from the payload. Additionally, many sites utilize techniques such as domain

fronting, CDN usage, and dynamic subdomains, further complicating domain name or protocol-based filtering efforts. As a result, even if a site is added to the Layer7 list, access to the site can still succeed, whether through normal connections or stealth mode. This demonstrates that Layer7-based filtering methods have limitations when dealing with modern web architectures and should be combined with other methods such as DNS filtering or IP-based blocking for more effective results.

3.11 QOS Results from Web Filtering

Before implementing web filtering, a Quality of Service (QoS) measurement was conducted for 10 minutes to obtain an overview of network performance under normal conditions. Based on the analysis, the network throughput reached 335,600.96 kbps, calculated from the total data of 25,180,132 bytes transmitted over a period of 600.147 seconds (10 minutes). Packet loss was recorded at 2.7623%, with 1,210 packets lost out of a total of 43,800 packets sent. The average delay or packet latency was 13.7 milliseconds, calculated by dividing the total delay by the number of successfully received packets. Meanwhile, the jitter, which indicates the variation in delay between packets, was recorded at 16.93 milliseconds, based on the total delay variation of 720.90 seconds relative to the number of effective packets. These results serve as a baseline before web filtering is implemented, enabling the impact of filtering policies on network quality to be evaluated objectively.

Table 7. Qos Results Before Web Filtering

No	Parameter QoS	Before	Category	Index
a.	Throughput	335.60 kbps	Very good	4
b.	Packet Loss	2.76%	Good	3
c.	Delay	13.7 ms	Very good	4
d.	Jitter	16.93 ms	Good	3

Based on the results captured during the 10 minutes after applying web filtering, QOS tests such as throughput, packet loss, delay, and jitter were obtained as follows.

a. *Throughput : !tcp.analysis.flags &&tcp*

$$\frac{number\ of\ bytes}{Time\ Span} = \frac{28.512.000}{600.147} = 47.504\text{byte} \times 8 = 380.032\ \text{kbps}$$

b. *Packet Loss : !tcp.analysis.lost_segment*

$$\frac{Lost\ Package}{Total\ Package} \times 100\% = \frac{720}{44{,}000} \times 100\% = 1{,}636\ \%$$

c. *Delay : !tcp.analysis.flags*

$$Delay = \frac{Total\ Delay}{Package\ received} = \frac{528}{43{,}280}$$

$$Average\ delay = 0.0122 \times 1000\ \text{second} = 12{,}2\ mili\ second$$

d. *Jitter*

$$Jitter = \frac{total\ delay\ variation}{(Total\ package-1)} = \frac{526{,}2\ \text{second}}{(43{,}800-1{,}210)} = 526{,}2/42.590 = 0{,}01236$$

$$Jitter = \quad = 12{,}15\ \text{mili second}$$

Table 8: Qos Results After Web Filtering

No.	Parameter QoS	Before	Category	Index
a.	Throughput	380.160 kbps	Very good	4
b.	Packet Loss	1.636%	Good	4
c.	Delay	12,2 ms	Very Good	4
d.	Jitter	12,15 ms	Good	3

Table 9: Comparison of Qos Results After and Before Web Filtering

No.	Parameter QoS	Before	After	Difference	Change
a.	Throughput	335.60 kbps	380.16 kbps	+44.56 kbps	Up
b.	Packet Loss	2.76%	1.636%	−1.12%	Down
c.	Delay	13.7 ms	12,2ms	−1.5 ms	Down
d.	Jitter	16.93 ms	12.15 ms	−4.78 ms	Down

After web filtering was applied for 10 minutes, there was a significant improvement in network quality. Throughput increased by 44.56 kbps, from 335.60 to 380.16 kbps, indicating better data transmission efficiency. Packet loss decreased by 1.12%, from 2.76% to 1.6%, indicating a more stable connection. Delay also decreased by 1.5 ms, from 13.7 ms to 12.2 ms, resulting in faster network response times. Meanwhile, jitter decreased by 4.78 ms, from 16.93 ms to 12.15 ms, indicating more consistent packet arrival times. Overall, web filtering had a positive impact on network performance.

4. Conclusion

Based on the results of research and implementation of a content filtering system using the Layer 7 Protocol Filtering method on MikroTik RouterOS devices, the following conclusions can be drawn:

1. Of the six pornographic websites tested, only four were successfully blocked by the system. Meanwhile, of the 17 online gambling websites tested, only nine were successfully blocked. This shows that the effectiveness of this method has not yet reached the maximum level of filtering, with a success rate of around 66.67% for pornographic websites and 52.94% for online gambling websites.

2. The implementation of web filtering also has a positive impact on overall network quality. A 10-minute test showed an improvement in Quality of Service (QoS) parameters, with throughput increasing from 335.60 kbps to 380.16 kbps (+44.56 kbps), packet loss decreasing from 2.76% to 1.64% (−1.12%), delay decreased from 13.7 ms to 12.2 ms (−1.5 ms), and jitter decreased from 16.93 ms to 12.15 ms (−4.78 ms). These improvements indicate that content filtering helps stabilize network traffic by reducing the load from accessing non-priority sites.

5. Suggestions

Based on the results of the research and testing conducted, there are several recommendations that can be made to improve the effectiveness of content filtering systems, particularly in addressing the challenges posed by the evolving web technology landscape, which is increasingly shifting toward the use of HTTPS protocols. Given that the Layer 7 Filtering method used in this study has limitations in reading encrypted traffic, it is recommended to use additional devices such as firewalls or external proxies that support SSL inspection (HTTPS filtering) in large-scale implementations or network environments requiring stricter and more comprehensive access control. These devices enable analysis of TLS/SSL connections, allowing domains or content protected by encryption to be effectively filtered. Additionally, integration with external DNS Filtering services can serve as a practical and efficient alternative to block access to inappropriate websites. Some recommended DNS Filtering services include AdGuard DNS, Cloudflare, and Cisco Umbrella (OpenDNS). These services provide filtering based on content categories and can be configured directly within the MikroTik DNS settings without requiring additional devices. By combining these methods, network administrators can create a more reliable system for filtering harmful or inappropriate content while addressing the limitations of conventional Layer 7 Filtering methods.

References

[1] Suryanto, D., & Rahman, H. (2022). Transformasi Digital dalam Pelayanan Publik di Era Revolusi Industri 4.0. Jurnal Administrasi Publik, 14(2), 55–66.

[2] A. Rahmat, “Implementasi Web Filtering pada MikroTik Router untuk Keamanan Jaringan,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 8, no. 2, pp. 123–130, 2021.

[3] S. Prasetyo dan D. Sari, “Metode Observasi dan Wawancara dalam Pengumpulan Data Penelitian Teknologi Informasi,” Jurnal Penelitian Komunikasi dan Pembangunan, vol. 23, no. 1, pp. 45–52, 2020.

[4] L. Kurniawan, “Analisis QoS (Quality of Service) Jaringan Menggunakan Parameter Throughput, Delay, Jitter dan Packet Loss,” Jurnal Teknologi Informasi, vol. 10, no. 1, pp. 15–22, 2022.

[5] R. K. Putri and S. N. Aulia, "Penggunaan Layer 7 Protocol pada MikroTik untuk Penyaringan Konten Berbasis URL," *Jurnal Ilmiah Teknologi Informasi Terapan*, vol. 10, no. 1, pp. 18–24, 2022.

[6] F. Hidayat and L. Kurniawan, "Analisis Kinerja Jaringan Menggunakan Metode Quality of Service (QoS) pada Router MikroTik," *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 1, pp. 55–62, 2020.

[7] R. Prasetyo, A. H. Putra, and D. P. Lestari, "Penerapan Web Filtering dan Layer 7 Protocol di MikroTik untuk Membatasi Akses Internet," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 4, pp. 321–328, 2019.

[8] A. Nugroho and M. P. Rahayu, "Implementasi Firewall pada MikroTik RouterOS untuk Keamanan Jaringan LAN," *Jurnal INFOKOM*, vol. 9, no. 2, pp. 8

[9] R. Prasetyo, A. H. Putra, and D. P. Lestari, "Penerapan Web Filtering dan Layer 7 Protocol di MikroTik untuk Membatasi Akses Internet," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 4, pp. 321–328, 2019.7–94, 2021.

[10] D. Yuliana and T. R. Sihombing, "Pengaruh Penerapan Firewall MikroTik terhadap Produktivitas Pengguna dalam Lingkungan Kerja," *Jurnal Teknologi dan Riset Terapan*, vol. 3, no. 3, pp. 25–33, 2021.

[11] M. S. Firmansyah, "Evaluasi Kinerja Firewall Menggunakan Router MikroTik Terhadap Keamanan Jaringan," *Jurnal Elektro dan Telekomunikasi Terapan*, vol. 4, no. 2, pp. 42–50, 2020.