YAYASAN AKRAB PEKANBARU
Akrab Juara : Jurnal Ilmu-ilmu Sosial
Volume 11 Nomor 1 Edisi Februari 2026 (579-589)

45

IMPLEMENTATION OF LOCAL AREA NETWORK SECURITY USING THE SITE ACCESS BLOCKING METHOD ON LAYER 7 PROTOCOL MIKROTIK RB 941-2ND

Arina Selawati, Rizka Dahlia
Universitas Bina Sarana Informatika
(Naskah diterima: 1 January 2026, disetujui: 28 January 2026)

Abstract

Computer networks are a highly sought-after service today. A computer network is a connection that allows two or more devices to physically or logically communicate with each other to exchange data and information. Managing a local area network (LAN) is one alternative solution to this problem to achieve optimal service. A key consideration in managing a local area network is network security, which involves regulating and restricting user access to websites. This aims to improve security and prevent network access from heavy traffic, caused by unproductive website access during work hours, excessive bandwidth usage, and the threat of cyberattacks. One network device that has features for implementing or activating computer network security is the MikroTik router. MikroTik firewalls contain Layer 7 Protocols, which contain parameters such as protocol, destination port, source port, and content. If traffic separation is not possible, we can consider using the Layer 7 Protocol or L7-protocol feature.
Keywords: *Computer Networks, Network Security, MikroTik, Layer 7 Protocol*

Abstrak

Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan Komputer merupakan koneksi yang memungkinkan dua atau lebih device terhubung satu sama lain secara fisik maupun secara logika saling berkomunikasi untuk bertukar data maupun informasi. Pengelolaan jaringan lokal (Local Area Network) merupakan salah satu alternatif penyelesaian masalah agar didapatkan layanan yang maksimal. Hal yang perlu diperhatikan dalam pengelolaan jaringan local adalah keamanan jaringannya dengan mengatur dan membatasi pengguna untuk mengakses situs/website, yang bertujuan untuk meningkatkan keamanan serta mencegah akses jaringan dari ramainya lalu lintas jaringan karena banyaknya yang mengakses website non produktif di jam kerja, penggunaan bandwith yang berlebihan dan bukan untuk produktifitas hingga ancaman dari serangan cyber. Salah satu perangkat jaringan yang memiliki fitu untuk melakukan atau mengaktifkan keamanan jaringan komputer adalah perangkat router mikrotik. Pada mikrotik didalam firewall terdapat Layer 7 Protocol berupa parameter-parameter seperti protokol, destination-port, source-port maupun content tidak mampu melakukan pemisahaan traffic, maka kita bisa mempertimbangkan untuk menggunkan fitur Layer 7 Protocol atau L7-protocol.
Kata Kunci: Jaringan Komputer, Keamanan Jaringan, Mikrotik, Layer 7 Protocol

I. INTRODUCTION

Computer networks are currently a much-needed service. They offer more benefits than stand-alone computers. They enable the shared use of data, software, and equipment, enabling workgroups to communicate more effectively and efficiently. A computer network is a connection that allows two or more devices to be physically or logically connected to each other and communicate to exchange data and information. Computer networks can have two, tens, or even millions of nodes. Hardware, software, and network problems are addressed to address these issues. Proper and accurate handling can reduce unwanted damage and thus improve effective performance. One type of computer network based on area is a Local Area Network (LAN), a computer network with a limited reach, such as a building, campus, office, or factory. A LAN is built with a minimum of two computers, each with high or low specifications. A LAN connects computers to other computers, even within a limited scope.

Local area network management is an alternative solution to problems to achieve maximum service. A crucial consideration in managing a local network is network security, ensuring users can access the network safely and in accordance with the regulations established for shared network use. Websites are currently a primary means of conveying information and providing digital services, both for individuals and institutions, and can be accessed through a computer network and the internet. However, websites also carry the risk of various cyberattacks that can damage data, disrupt systems, and cause harm to users. Therefore, it is important to conduct regular security testing on websites to identify system vulnerabilities and prevent potential losses caused by undetected security vulnerabilities.

Proxy Management Using Mikrotik with the Layer 7 Protocol and Mangle Methods. Despite all its advantages and convenience, the internet certainly has its downsides, one of which is the abundance of negative content accessible to anyone. The author is interested in creating a proxy server that can block negative websites using the MikroTik-based Layer 7 Protocol and Mangle methods.

Previous research has shown that content filtering techniques using firewall filter rules on a MikroTik RB941-2ND device effectively block access to content such as Instagram. The internet is distributed via LAN cable to user devices, and the results demonstrate that negative site filtering can be implemented in computer networks. This method helps administrators restrict specific access and monitor network traffic, thereby improving user security and productivity.

After reviewing and studying previous research, the author implemented Local Area Network (LAN) security by regulating and restricting user access to websites. This aims to improve security and prevent network access from heavy traffic due to the large number of people accessing non-productive websites during work hours, excessive bandwidth usage for non-productive purposes, and the threat of cyberattacks due to accessing unsafe websites or websites containing viruses. Network instability and bandwidth waste can be prevented by limiting user access rights. Therefore, this research focuses not only on improving network quality but also on strengthening security. Implementing a firewall is expected to reduce unnecessary bandwidth usage, especially during spikes in network activity due to access to sites or applications unrelated to user productivity. This is achieved by utilizing the Layer 7 protocol feature on the MikroTik RB941-2ND device to block sites on specified websites.

II. THEORETICAL STUDIES

A computer network consists of two or more interconnected computers. A computer network is defined as a network of computers or a collection of terminals connected to one or more computers. A computer network is generally a network that allows nodes to share resources. The history of computer networks began with time-sharing networks, where terminals were connected to a central computer called a mainframe. A computer network is a technology that allows computer devices to connect and communicate with each other. Computer networks also allow devices to share resources and information, thereby increasing user efficiency and productivity.

A Local Area Network (LAN) is a privately owned network within a building or campus, up to several kilometers in size, designed to share resources and exchange information. Furthermore, a Local Area Network (LAN) can be defined as a computer network with a very small or limited network coverage area. For example, a computer network in an office, school, home, or within a single room.

The more extensive the use of computer networks, the greater the potential security threats. Therefore, network security is crucial for maintaining data confidentiality, integrity, and availability. Furthermore, network security is an effort to secure network performance and processes, preventing unauthorized use and interference with system resources.

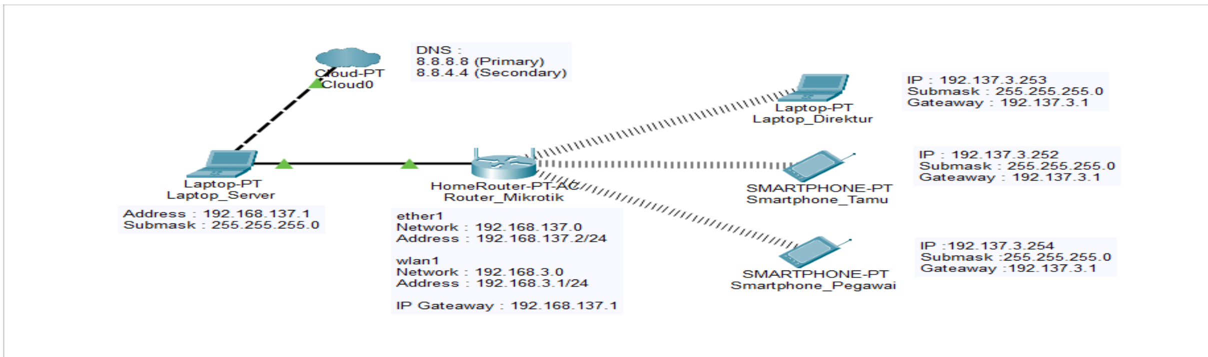
One network device that has features for enabling computer network security is the MikroTik router. MikroTik is a Latvian company founded in 1996 to develop routers and wireless ISP systems. MikroTik now provides hardware and software for internet connectivity in most countries worldwide. In 1997, the RouterOS software system was launched, providing stability, control, and extensive flexibility for all types of data interfaces and routing. Then, in 2002, MikroTik developed its own hardware under the RouterBOARD brand. MikroTik includes features such as a firewall, which protects the network from external threats by determining whether data packets can enter and exit the network. Because proxies have firewall features that allow network service providers to utilize them, their use on the network is very beneficial. In Mikrotik, the firewall contains a Layer 7 Protocol containing parameters such as protocol, destination port, source port, and content, which are unable to separate traffic. Therefore, we can consider using the Layer 7 Protocol or L7-protocol feature. Layer 7 Protocol is a feature that will examine data at layer 7 of the OSI model. Of course, there are several consequences if you have to use this Layer 7 Protocol feature. It is enough to know that information to be sent to the destination computer will be processed into data. This process of converting information into data occurs at layer 7 of the OSI model. After that, the data will be wrapped (encapsulated) with some additional information called a header. The header itself consists of several fields such as source-address, destination-address, protocol, source-port, and destination-port parameters, which are some of the fields added to the data. Data that has been added to the header is with a packet.

III. RESEARCH METHODS

In this research, the author carried out several stages: problem identification, planning, implementation, and evaluation. The identification stage was conducted to identify network needs and constraints by studying references and previous research. After that, an appropriate solution was designed in the planning stage. Implementation was carried out by installing and configuring network devices. After implementation, the author conducted periodic evaluations to test the results and ensure the network was running properly and was able to address the problems identified.

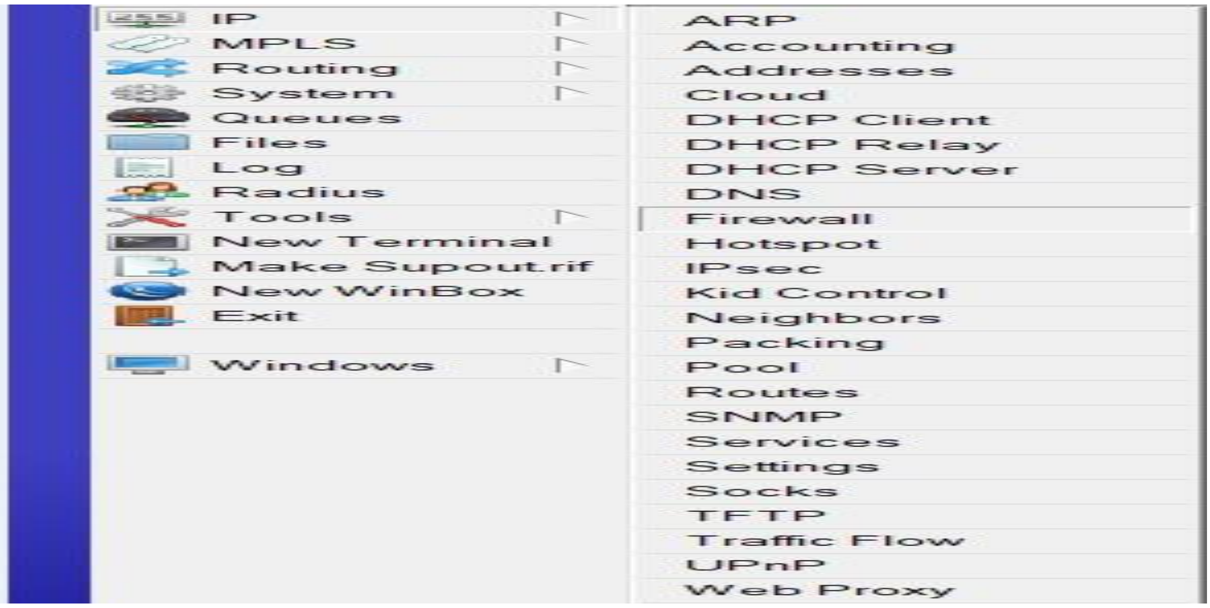
IV. RESEARCH RESULTS

Based on the results of the analysis and implementation of local area network security with the site access block method on the Mikrotik RB 941-2nd layer protocol that the author did in this study, it has several results, namely increasing the security of the local area network by setting access to any sites/websites that are not permitted to be accessed by clients or network users. By configuring site blocks on the layer 7 protocol and registering websites/sites that are not allowed to be accessed with the desired time limit. The network scheme that the author applied in this study is as follows.



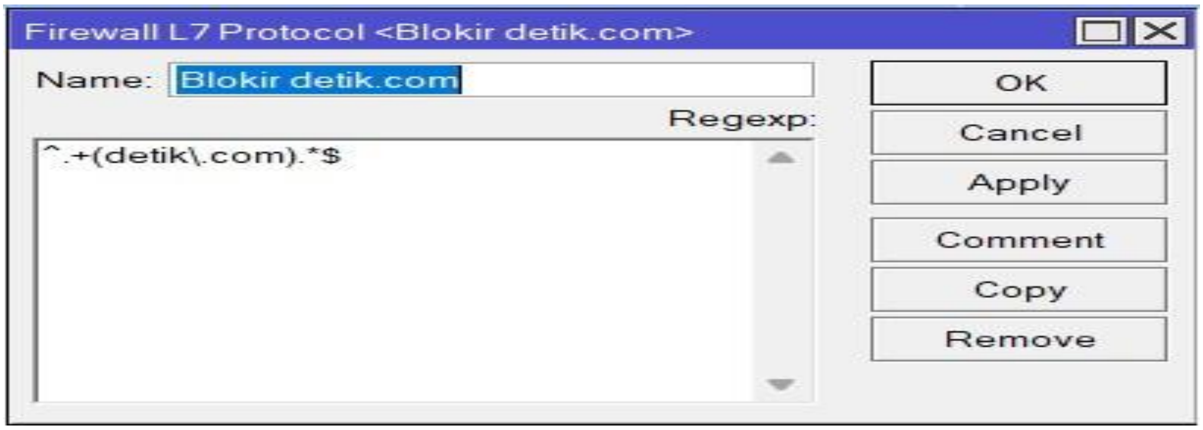
Network Schematic

The configuration steps taken by the author to demonstrate the analysis and implementation of local area network security using the site access block method on the Mikrotik RB 941-2nd Layer 7 protocol in the network schematic above are as follows:



Entering the Firewall Menu on Mikrotik

The steps above demonstrate the initial steps for configuring the site access blocking method on the Layer 7 protocol on the Mikrotik RB 941-2nd. This is done by entering the firewall menu. Then, select the Layer 7 Protocol tab and add the website you wish to block/restrict access to by typing the regexp ^.+(WEBSITEADDRESS\.COM).*$ as shown in the image.


Firewall L7 Protocol <Blokir detik.com>

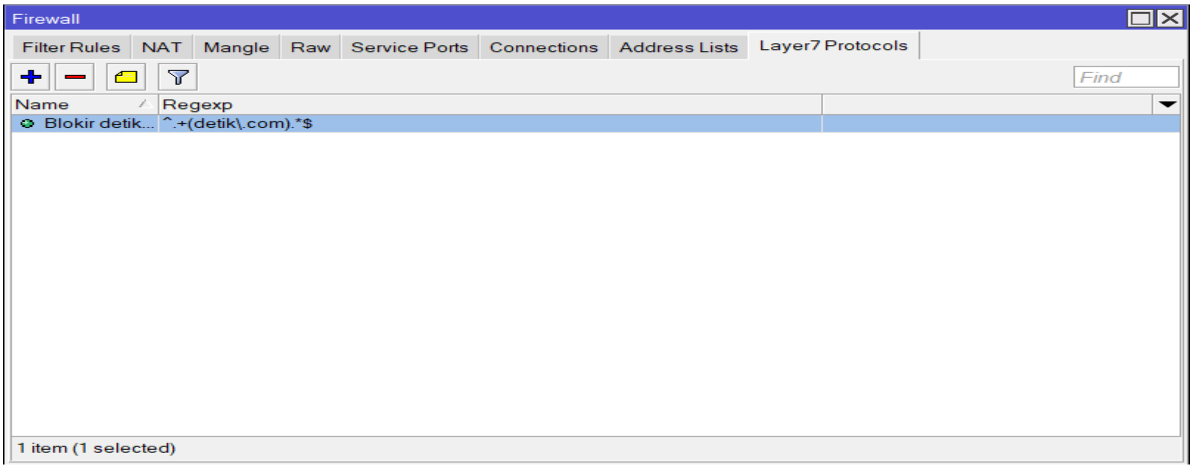
Name: Blokir detik.com

Regexp:

```
^.+(detik\.com).*$
```

Registering a website with RegExp

Once you've selected the website you want to block/restrict access to, the Layer 7 protocol menu will display all the websites you've listed.

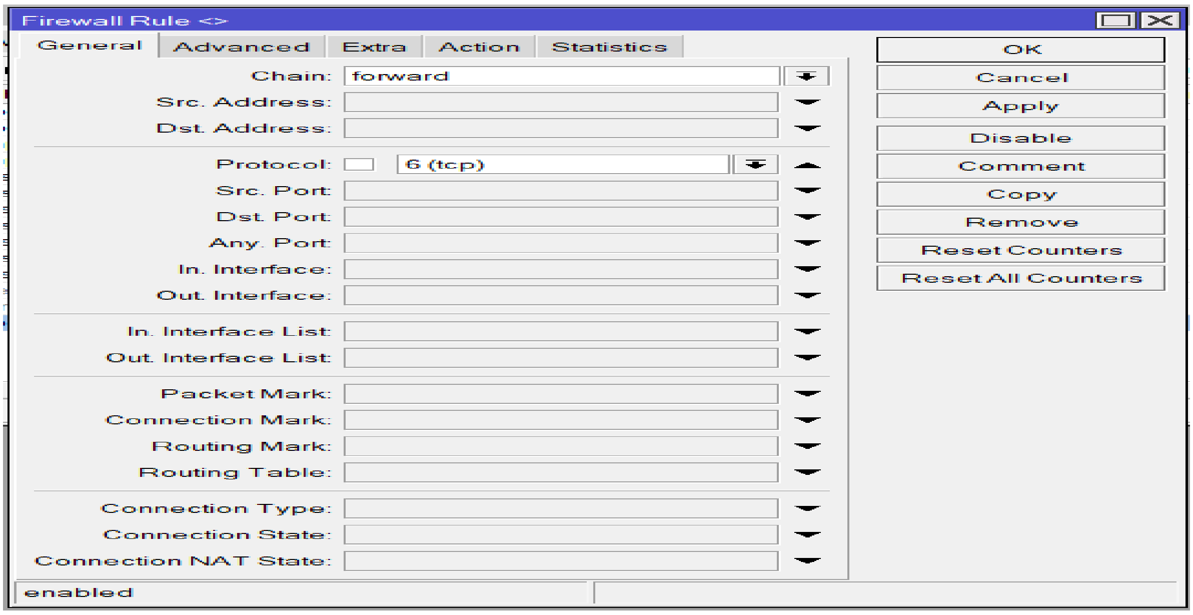


Name	Regexp
Blokir detik...	^.+(detik\.com).*$

1 item (1 selected)

Results from the website registered in regexp

Then, after the website you want to register in the Layer 7 protocol, continue by configuring the Filter Rules > then click "+" > Chain: forward > Advance > click Layer 7 Protocol. It will automatically populate if there is only one website > Action: drop > Apply and OK

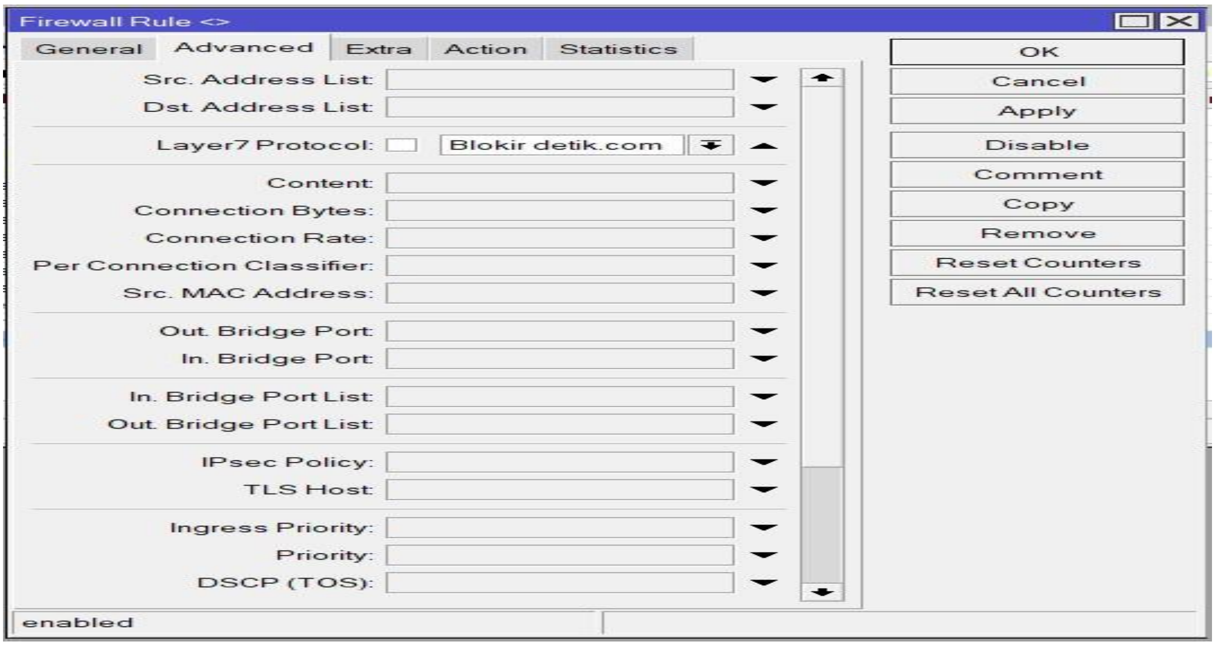


Chain: forward

Protocol: □ 6 (tcp)

enabled

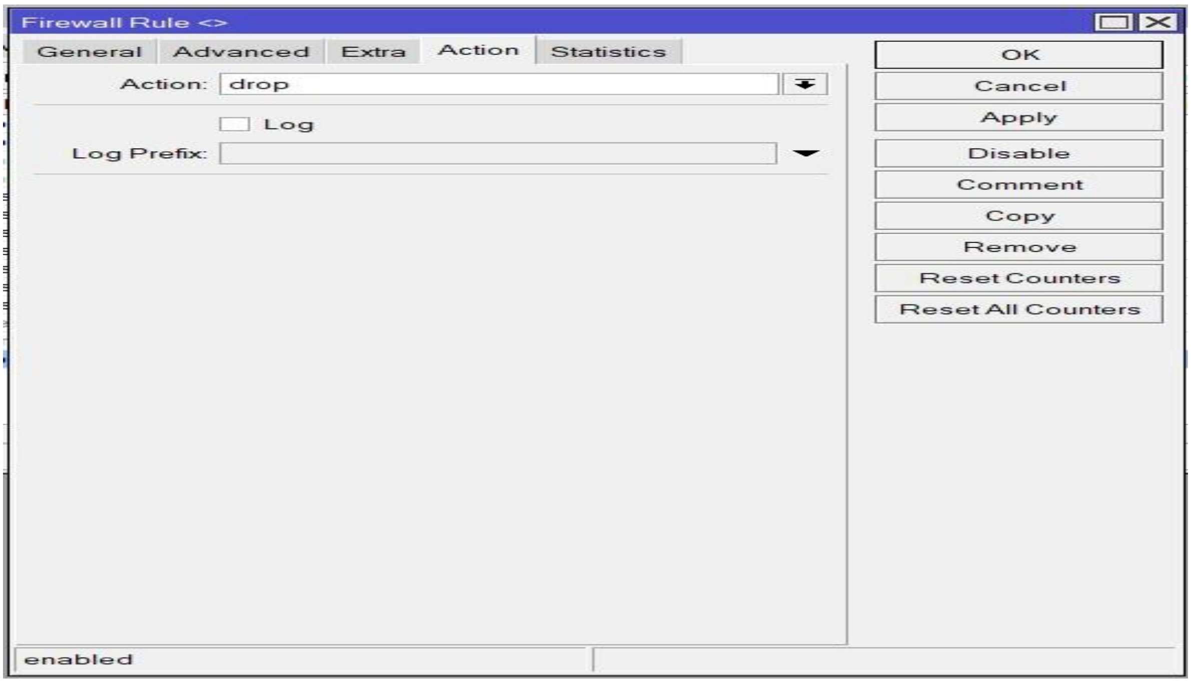
Configuration of filter rules in the general section



Layer7 Protocol: □ Blokir detik.com

enabled

Configuration in the filter rules in the advanced section



Action: drop

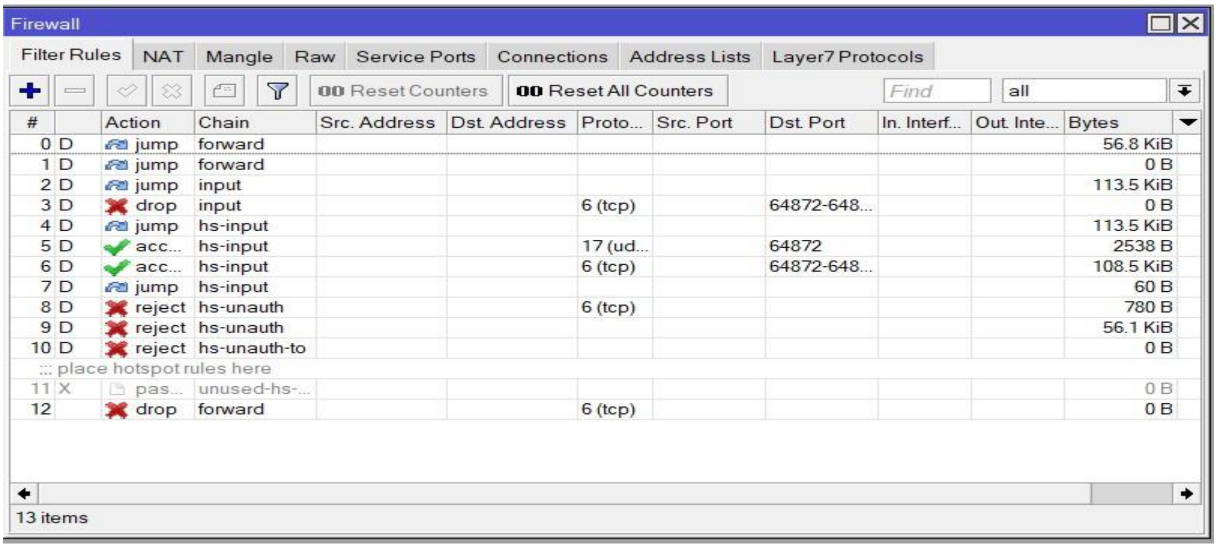
□ Log

Log Prefix:

enabled

Configure the filter rules in the action section

This configuration is used to block access to websites registered in the Layer 7 protocol tab. After completing this step, the MikroTik filter rules menu will display all websites registered in the Layer 7 protocol tab with the assigned access.

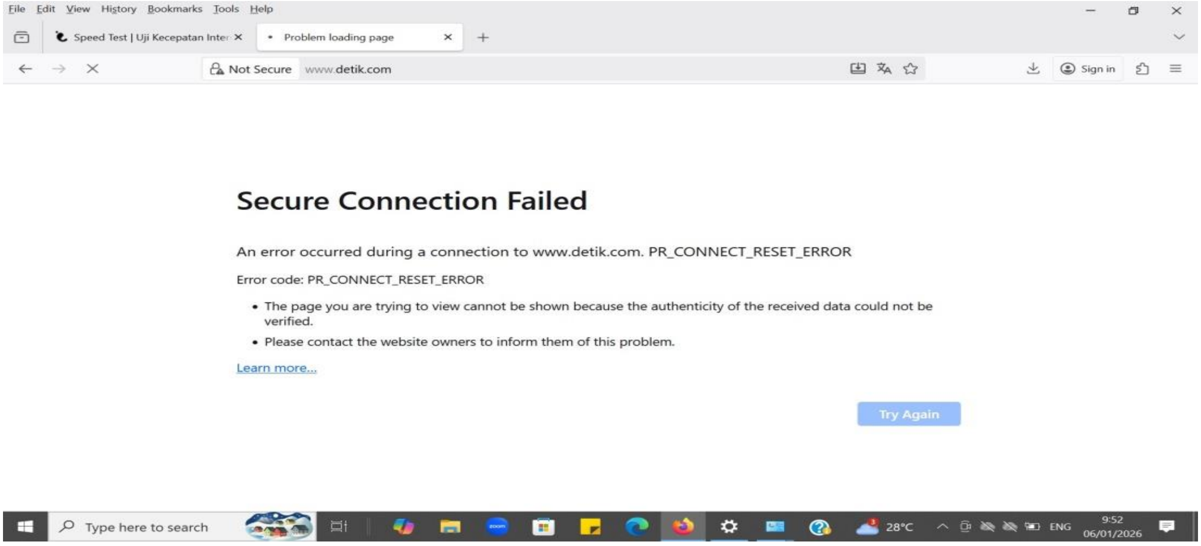


#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interf...	Out. Inte...	Bytes
0	D	jump	forward								56.8 KiB
1	D	jump	forward								0 B
2	D	jump	input								113.5 KiB
3	D	drop	input			6 (tcp)		64872-648...			0 B
4	D	jump	hs-input								113.5 KiB
5	D	acc...	hs-input			17 (ud...		64872			2538 B
6	D	acc...	hs-input			6 (tcp)		64872-648...			108.5 KiB
7	D	jump	hs-input								60 B
8	D	reject	hs-unauth			6 (tcp)					780 B
9	D	reject	hs-unauth								56.1 KiB
10	D	reject	hs-unauth-to								0 B
::: place hotspot rules here											
11	X	pas...	unused-hs-...								0 B
12		drop	forward			6 (tcp)					0 B

13 items

Configuration results in the filter rules action section

After all configurations have been completed, the next step is to verify whether the configuration was successful. This can be done by accessing the blocked website in the user's/client's browser.



Secure Connection Failed

An error occurred during a connection to www.detik.com. PR_CONNECT_RESET_ERROR

Error code: PR_CONNECT_RESET_ERROR

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

Try Again

Configuration test results

As seen in the image above, the website registered in the Layer 7 protocol tab on MikroTik is no longer accessible to users/clients on the local area network we created. Therefore, we can conclude that the configuration was successful and that the site blocking was successful.

V. CONCLUSION

Based on the results of the implementation of local area network security with the site access block method on the Mikrotik RB 941-2nd layer 7 protocol that the author has done, the results obtained that the configuration carried out was successful in regulating website access that can be accessed by network users/clients. So that traffic on the network can run well, websites accessed by users/clients can be measured, in addition, this configuration can also reduce excessive bandwidth usage because there are no users/clients who can access heavy websites and interfere with network productivity. And when unnecessary/unnecessary website access is no longer given access or is blocked, it has an impact on the network becoming more secure because users can no longer access dangerous sites/websites or carry viruses that can interfere with network performance.

REFERENCES

Deagama M, Antariksa S, Aranta A, Made I, Wiweka H, Ganiwa J. ANALISIS JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) DI RUMAH SAKIT UNRAM. JBegaTI. 2022;3(2):201–12.

Daniswara FJ, Voutama A. SIMULASI UJI KEAMANAN JARINGAN WINDOWS 7 BLOKIR AKSES SITUS DENGAN METODE LAYER 7 PROTOCOL BERBASIS MIKROTIK DALAM VIRTUALBOX. JITET (Jurnal Inform dan Tek Elektro Ter. 13(3):313–20.

Syam Basri Khalid, Hairul Fahmi MTAZ. IMPLEMENTASI PROXY SERVER MENGGUNAKAN FITUR LAYER 7 PROTOCOLS MIKROTIK DI STMIK LOMBOK. ETIK (Jurnal Elektron Terap dan Ilmu Komputer). 2025;2(1):21–31.

Yansen Sianhar M. PENERAPAN FIREWALL BERBASIS MIKROTIK DALAM OPTIMALISASI JARINGAN DI SEKOLAH MENENGAH KEJURUAN. J Inform Teknol dan Sains. 2025;7(2):868–77.

Amala R, Mewengkang A, Djamen AC. Analisa dan Perancangan Jaringan Komputer di SMKN 2 Bitung. EduTIK J Pendidik Teknol Inf dan Komun. 2023;Volume 3 N(April):260–9.

Ali M, Latifah F. IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL. J Inf Syst Applied, Manag Account Res. 2021;5(2).

Hafiz S, Ginting N, Martin A, Chyan P, Nirawana WS, Nadzirin M, et al. Pengantar Jaringan Komputer PT. MIFANDI MANDIRI DIGITAL. 2023.

Riadi I, Studi P, Informasi S, Dahlan UA. Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. JUSI. 2011;1(1):71–80.

Setiawan O, Syahroni M, Muhammad. IMPLEMENTASI FAILOVER DENGAN METODE RECURSIVE GATEWAY PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS ROUTER MIKROTIK RB951UI. J TEKTRO. 2021;05(02).

Pratomo AB. PENGEMBANGAN SISTEM FIREWALL PADA JARINGANKOMPUTER BERBASIS MIKROTIK ROUTEROS. 2023;1(2). Available from: https://doi.org/10.59688/bufnets

Saputra K, Ariyadi T. IMPLEMENTASI AUTOMATIC FAILOVER JARINGAN LANMENGGUNAKAN MIKROTIK DI CV MAKMUR ABADI.

Yuliansyah E, Saputra S, Ali I. IMPLEMENTASI REDUNDANT LINK UNTUK MEMINIMALISIR DOWNTIME DENGAN METODE FAILOVER (STUDI KASUS:

PT KEMUNING PERSADA). JUPIKOM [Internet]. 2022;1(3). Available from: http://ejurnal.stie-trianandra.ac.id/index.php/jupkomHalamanUTAMAJurnal:http://ejurnal.stie-trianandra.ac.id/index.php

Shomad A, Akbar Y, Mulyana DI, Informatika T, Tinggi S, Komputer I, et al. Implementasi Pembatasan Akses Sosial Media Menggunakan Layer 7 Protocol Pada Perangkat Mikrotik DI SMK IDN. INFORMATICS Educ Prof. 2022;7(1):27–38.

Pratama YA, Gratianus F, Larosa N, Gea A. Analisis Efektifitas Fungsi Fitur PCQ Simple Queue Dan Fitur Layer-7 Protocol Pada Mikrotik Router (Studi Kasus SMK Imelda). J Ilm Tek Inform. 2023;3(1):66–74