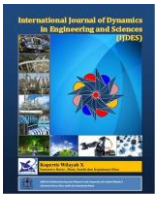
INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 6, No. 1, Month 2021
e-ISSN: 2502-0692



DESIGN AND BUILD IMPLEMENTATION OF FILTER RULES FOR NETWORK SECURITY WITH MIKROTIK ROUTERBOARD

Mohd. Siddik [1], Suparmadi [2]
[1] STMIK Royal
Kisaran, Asahan Regency, Indonesia
[2] STMIK Royal
Kisaran, Asahan Regency, Indonesia

doi. 10.22216/jod.v6i2.852
*Correspondence should be addressed to mohdsiddiik@gmail.com

Article Information

Submitted :
25 March 2021

Accepted :
18 April 2021

Published :
01 May 2021

Abstract

Internet is a computer network technology that is needed by every user today. With internet technology, the information needed can be quickly accessed by users around the world, including in Indonesia. Internet users in Indonesia are the largest in Southeast Asia. Government and private agencies and even the business and industrial world cannot be separated from internet technology. The application of network security is currently still mostly using a simple security system that is only by activating the firewall on the modem. With this, it is still considered not optimal because there are many users in one network. So to optimize it requires a good network security system as well. This study aims to design and optimize a network security system by using a Mikrotik routerboard as network management hardware. By activating the filtering rule as a block and restricting user access. The results of this study are designs that can be used to optimize computer network security systems.

Keywords: Network security, Computer Network, Mikrotik

1. Introduction

Internet is a computer network technology that is needed by every user today. With internet technology, the information needed can be quickly accessed by users around the world, including in Indonesia. Internet users in Indonesia are the largest in Southeast Asia. Government and private agencies and even the business and industrial world cannot be separated from internet technology, so data exchange traffic will often occur and this will require a good level of data and network security. The amount of data and information exchange that occurs requires a good network security system as well. Currently, the use of internet network technology for network management is still not widely implemented, the management of internet network security systems still relies mostly on modem devices provided by ISP services. So this will cause data security problems and the internet network. So one solution to prevent data theft and even data hacking is to perform network management using a Mikrotik routerboard.

A computer network is an "interconnection" between 2 or more autonomous computers, which are connected by wired or wireless transmission media. Computer networks are also telecommunications networks that allow computers to communicate with each other by exchanging data[1].

Computer network security is a series of processes in systematic network management to prevent and identify unauthorized use of a computer network[2]. A firewall is a service of a computer network security system that can protect against viruses, malware, spam, and

attacks. Attacks on information system security (security attacks) today often occur[3].

Network security is one of the measures to protect the data on the server, apart from using the data encryption method, there is also one technique used to secure the network, namely by using the DMZ (Demilitarized Zone) technique[4].

This study examines the development of a wireless network that utilizes a PC router with a Mikrotik Router OS v.5.20. hereby shows that a wireless network with a proxy router OS v.5.20 on a PC router to configure bandwidth management, web filtering, and user management can secure and optimize the functions of the existing wireless network. For this reason, it is necessary to increase bandwidth capacity and improve network security from attacks such as hotspot hacking[5].

Research on Network Security Systems using Cisco AnyConnect with the Network Access Manager Method concluded that the use of a network security system using Cisco ISE with the network access manager method was actually able to help implement IT Policy standards at PT Lintasarta. The initial stages are to strengthen or anticipate network security systems for IT The policy at PT Lintasarta is to standardize security for each Layer 2 network device that previously used an unmanaged access switch to become a managed access switch from Cisco which already supports the implementation of ISE features[6].

Research on network security simulations that are tailored to the network topology and take advantage of various features available on Mikrotik such as firewalls and network security support features. In general, this research produces firewall configuration, service port management, and filter configuration for Bridge. By implementing four firewall configurations, it is functioned to block user activity or attacks from outside that can endanger the network security system[7].

Network security by using a combination of username and password to replace digital certificates in Extensible Authentication Protocol-Tunelled Transport Layer Security (EAP-TTLS) can increase user mobility, because users do not need to add digital certificates to log into hotspots. EAP-TTLS authentication has better capabilities which are added with MD5 encryption on MikroTIK hotspots so that users are comfortable logging into hotspots and make it easier for IT employees from Idoop Hotel to manage large numbers of users[8].

Another study, Analysis of Wireless Network Security at Al Firdaus Middle School concluded that wireless network security at Firdaus High School already uses WPA/WPA-level security with this network security is more secure[9].Further research Computer network security is a problem that must be considered by users. In addition, the development of computer network security technology must continue to be carried out as soon as possible and reduce technically illegal elements. Various technical breakthroughs should be realized as soon as possible, and security protection measures should also be improved[10].

2. Method

In this study, the method used in designing the Implementation of Filter Rules for LAN Network Security based on Mikrotik Routerboard using the Network Development Life Cycle (NDLC) development model. Where in the application of this model can be seen in the following figure.

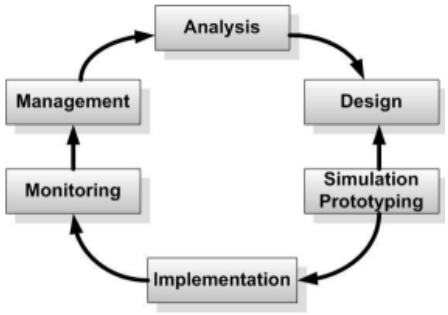


Figure 1. Network Development Life Cycle

1. Data Collection

At this stage of data collection by looking at reading journals related to network security.

2. Identification and Analysis

This stage is how to anticipate the occurrence of unauthorized users who can harm network users. The analysis was carried out by descriptive method. The data were collected, compiled, grouped, and analyzed in order to obtain an overview of the problems that occur in the network security system.

3. System Design

The design stage begins with designing a system analysis design for a network topology user analysis.

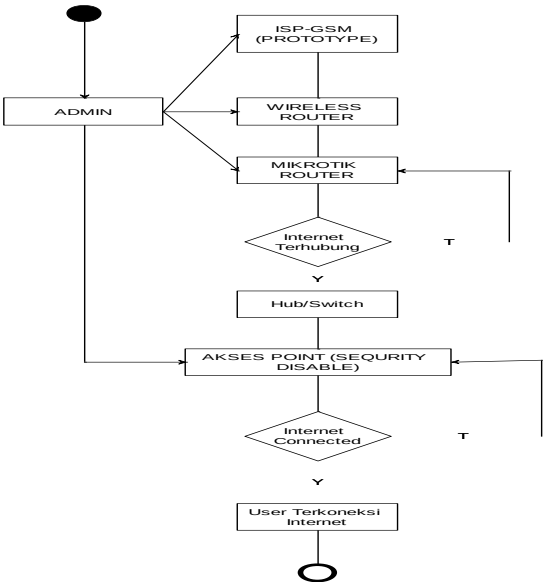
4. Implementation

This stage is testing the designed system. And see the results of the test.

3. Result and Discussion

A. System Flow Design

The design flow system design Implementation of Filter Rules for LAN



Network Security based on Mikrotik Routerboard starting from: Internet Service Provider Connection, Wireless Modem, Mikrotik Router, Users using different passwords.

Figure 2. Design System Analysis

B. User Analysis

Users who will use the network will get a different user code with other users. This is intended to facilitate the monitoring of user intruders.

Table 1. User Analysis

No	User	Information
1	Administrator	Responsible for network management, user passwords, monitoring users.
2	User	Users who use network services that have been provided.

C. Network Topology

The network design to be built can be seen in the following figure.

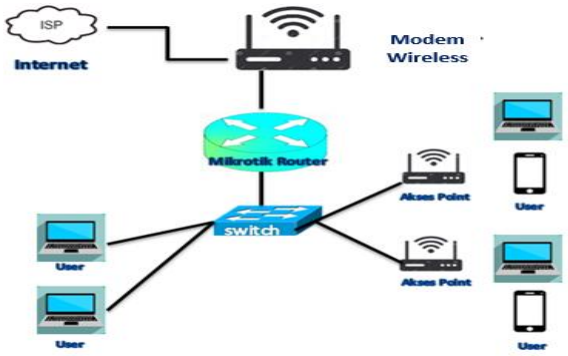


Figure 3. Network Topology Design

D. Mikrotik Router Configuration

Mikrotik router configuration starts from the interface, then by giving a name to each port. Ether1 Internet Connection, Port 2 Local.

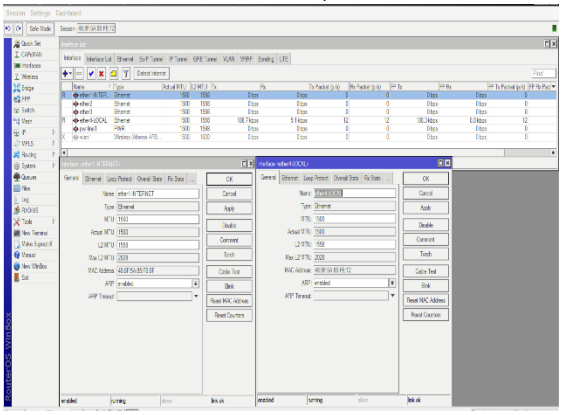


Figure 4. Interface Configuration

The next step is to configure the IP address of the Internet ISP Internet from the wireless router, namely 192.168.0.0/24. the ip address of the mikrotik router uses the ip address 192.168.0.2/24, and the local IP address is 192.168.97.254/21.

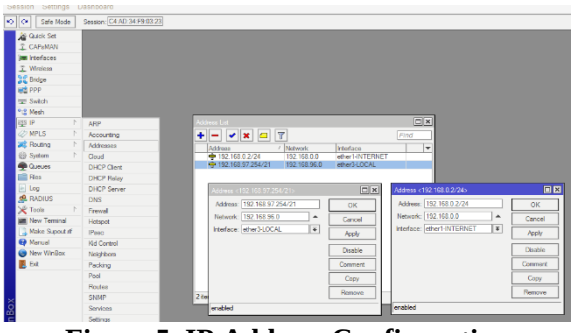


Figure 5. IP Address Configuration

Next, manage User Profiles, this is done in order to provide convenience in giving passwords to each user.

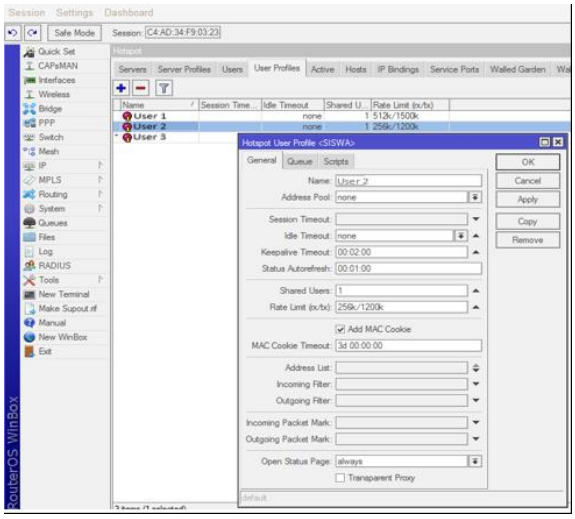


Figure 6. User Profile Management

The next stage is testing the user management that has been done.

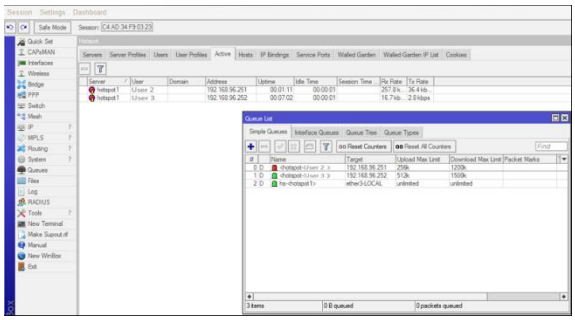


Figure 7. User Management Test

Then do filter rules, and block ports that are considered likely to be used by viruses, this management is carried out to improve network security.

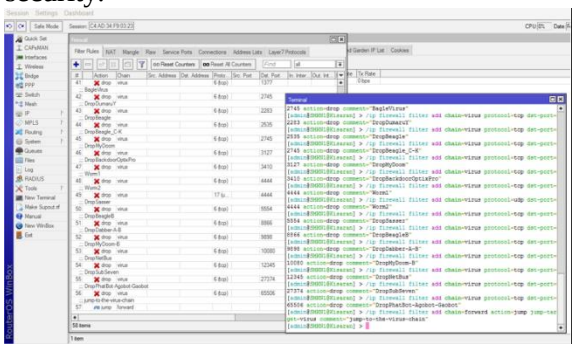


Figure 8. Filter Rule, Block Port

4. Conclusion

The conclusion obtained from the test results Each user has a different password to be able to access the internet, this makes monitoring easier, internet access is more stable. with filter rules, network security is better and more secure. The next stage in order to perfect this research, it is necessary to carry out direct implementation of network installations both in agencies and in direct companies.

References

[1] M. Syafrizal, *Pengantar jaringan komputer*. Yogyakarta: Andi, 2020.

[2] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, 'Keamanan Jaringan Komputer Pada Era Big Data,' J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[3] S. Arlis, "Analisis Firewall Demilitarized Zone Dan Switch Port Security Pada Jaringan," *J. KomtekInfo (Komput. Teknol. Inf.)*, vol. 6, no. 1, pp. 29–39, 2019.

[4] A. Z. Arifin, M. Agus Syamsul, "Bina Insan Lubuklinggau Menggunakan Teknik Demilitarized Zone (Dmz)," *J. Sist. Komput. Musirawas*, vol. 4, no. 1, pp. 19–24, 2019.

[5] M. Muhammad and I. Hasan, "Analisa Dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router Os V . 5. 20," vol. 2, no. 1, p. 2(1)., 2016.

[6] F. Dali, "Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager," *J. Ilmu Tek. dan Komput.*, vol. Vol.X, no. No. X, pp. 1–7, 2017.

[7] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, "Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta," *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.

[8] I Wayan Sukartayasa and I Putu Hariyadi, "Perancangan Keamanan Jaringan Authentication Login Hotspot Menggunakan Radius Server Dan Protokol Eap-Ttls Pada Mikrotik," *J. BITE*, vol. 1, no. 1, pp. 51–59, 2019.

[9] G. K. Dewi, M. K. Prof.Dr. Budi Murtiyasa, and M. S. Dedi Gunawan, S.T, "Analisa keamanan jaringan," *Univ. Muhammadiyah Surakarta*, p. 16, 2016.

[10] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, 'Keamanan Jaringan Komputer Pada Era Big Data,' J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.