Monitoring DNS Query With Pi-Hole Firewall Using Raspberry B+ Integrated With Microtik Router RB 931-2nd

[1]Hadi Syahputra
[1]Information System,
[1] Faculty of Computer Science,Putra Indonesia University YPTK Padang ,West Sumatera, Indonesia.

Abstract: This study aims to develop a system design that is integrated with a MICROTIK ROUTERBOARD connected to a PI HOLE that has been installed into the Ubuntu linux operating system that has been paired to a RASPBERRY B+ device that works to control the flow of data lines and disconnects both the client and the server and the action to skip , drop, reject, encrypt and log activity logs. The benefits obtained from the development of this system are to make it easier for admins in network management as well as incoming and outgoing traffic on the network. This research was conducted by designing, manufacturing and implementing system components including routerboard as a process controller, access point as a 2.4Ghz signal transmitter, Pi-hole is a program that allows everyone to create their own DNS server which acts as a sinkhole for the majority of advertisements and trackers on the internet.

IndexTerms **- Routerboard, Mikrotik, Hotspot, Pi Hole, Raspbbery B+, Ubuntu**

I. INTRODUCTION

The internet was originally developed by the United States in the mid-19th century, and was originally used for military purposes, but along with the development of internet technology, it has almost become a primary need because the services offered by the internet are more complete, communicative and pamper consumers in terms of internet access. Services that are accessed on the internet connected to a LAN (Local Area Network) or wirelessly or wirelessly are a DNS (Domain Name System) that maps a website address called host (hostnames) to a specific IP address number (IP Address) or vice versa. , so that the name of a page is easy to remember easily, from the address in the form of information stored (Records) by the Domain Register, DNS (Domain Name System) service providers, and web hosting service providers (Ahmad Fujianto, Indra Waspada, 2016).

Along with the development of technology, all technology companies in the world are competing to make the most sophisticated security systems in the world, but with very expensive costs and very difficult installations for the implementation of these devices, some newly developed companies are not able to create security systems on networks in Indonesia. companies both in terms of Servers, Databases and Wireless networks that they spread (Adityo Abdi Nugroho, Ahmad Shaugi, Yulius Dimas, 2013).

Based on the descriptions above and in order to realize the system design, the author would like to carry out a study entitled "MONITORING DNS QUERY WITH FIREWALL PI-HOLE USING RASPBERRY B+ INTEGRATED WITH MICROTIK ROUTER RB 931-2nd".

II. RESEARCH METHODOLOGY

The research methods carried out are as follows:

a. Research tool

In this research tool, the selection of related tools is carried out according to the tool made and to find out which Hotspots can be accessed by users, to analyze problems, and obtain the required information. And how the Pi-Hole Hotspot and Firewall can work according to their functions.

b. Library Research

This library research is carried out by reading, discussing, summarizing and drawing conclusions from books and journals about Hotspots and Raspberries, and Firewalls related to the analysis and design of network security systems to obtain materials that can scientifically be used as a basis for compiling this research.

c. Analysis

Based on the identification of the problems above, the researchers conducted data analysis first. This is so that problem solving can produce a new solution.

d. Hotspot and VPN Design

The design in the research to make Hotspots and Firewalls used in DNS Query Monitoring is based on certain considerations. This media tool must have criteria such as:

1. Each user's account has been registered in the user management on mikrotik
2. Filtering or Filtering content on the internet network
3. Prices are cheap and affordable by the community

4. The standard components used are easy to obtain.

Designed components are easy to manufacture. Easy to maintain and care for.

e. Testing

The planning for using the DNS Query Monitoring tool with the Pi-Hole Firewall using Raspbery B+ which is integrated with the Mikrotik Router RB 931-2nd is as follows:

1. Initial preparation is done by preparing the tools, as well as the auxiliary components used
2. The process of using an android smartphone is done by connecting to a network that has a firewall that has been designed
3. Calculate the quantity of the number of users who can connect to the Hotspot and the quality of the Hotspot signal.

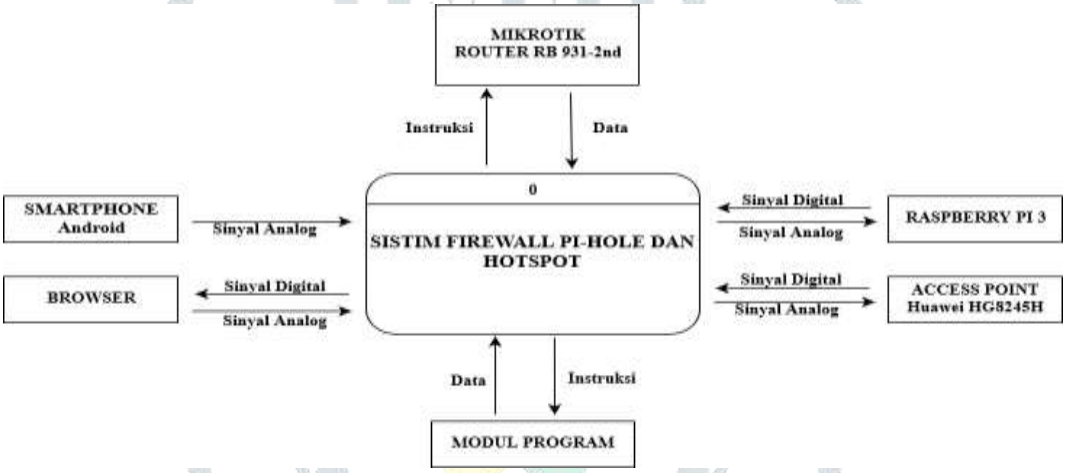
f. Hotspot and Pi-Hole Implementation

System implementation is the stage of putting the system so that it is ready for operation. Implementation aims to confirm the design modules, so that users can provide input to system development. At this stage the system design is carried out using the Linux operating system that has been installed with Pi-Hole as an additional firewall to increase security when using the internet.

III. RESULTS AND DISCUSSION

3.1 Context Diagram

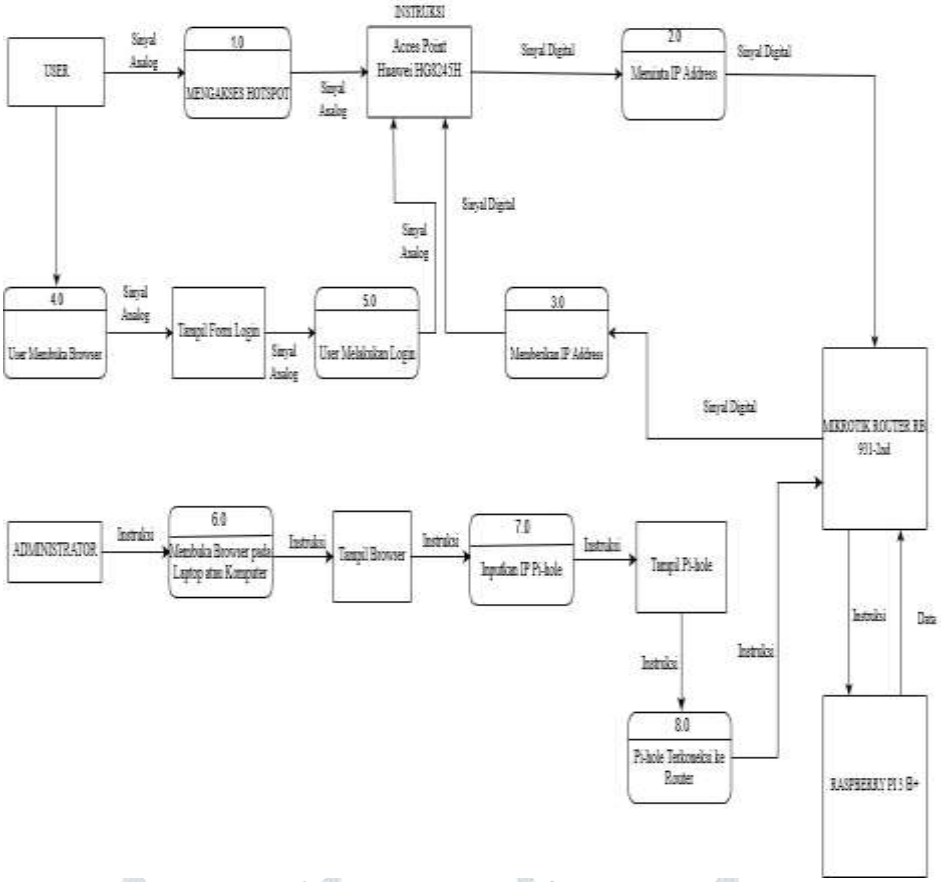
This sub-chapter is a description of each external entity as a whole which is described through a context diagram. Context diagram is a definition of the system to be designed that is comprehensive. This context diagram is used to facilitate the process of analyzing the system that is designed as a whole. Context diagrams function as media, which consists of a process and several external entities. The context diagram in question can be seen in Picture 1 below



Picture 1. Context Diagram Tool

3.2 Data Flow Diagrams

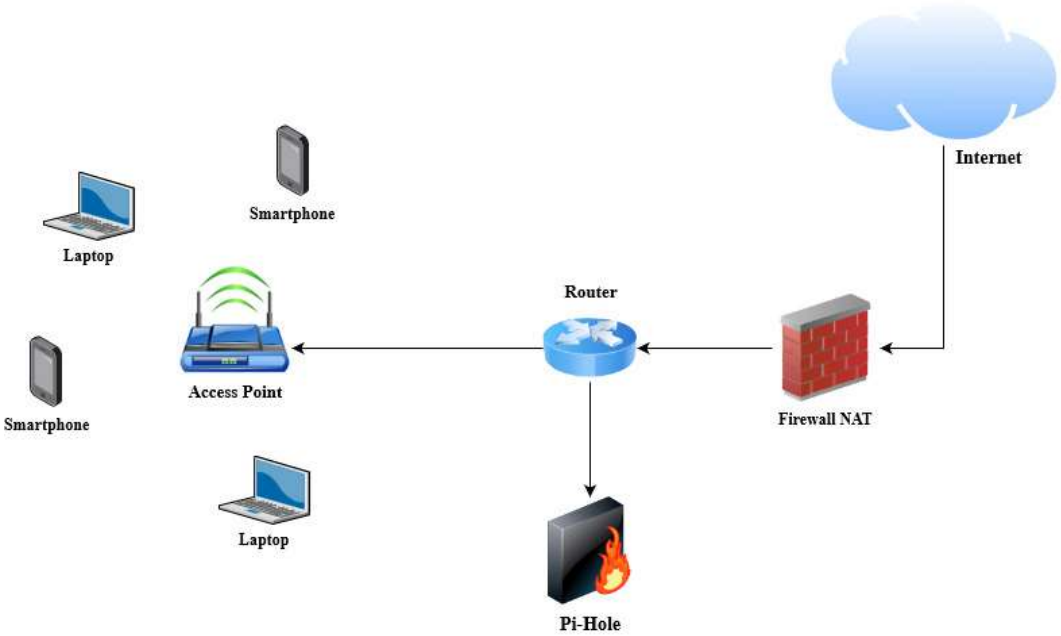
Data flow diagram is the flow of data from the tool made. The data flow diagram used is a level 0 data flow diagram because only one system has been developed. For more details can be seen in Picture 2



Picture 2. Data Flow Diagrams

3.3 Overall topology

Topology is a description of how the journey of data or information moves in a network is as follows, in Picture 3



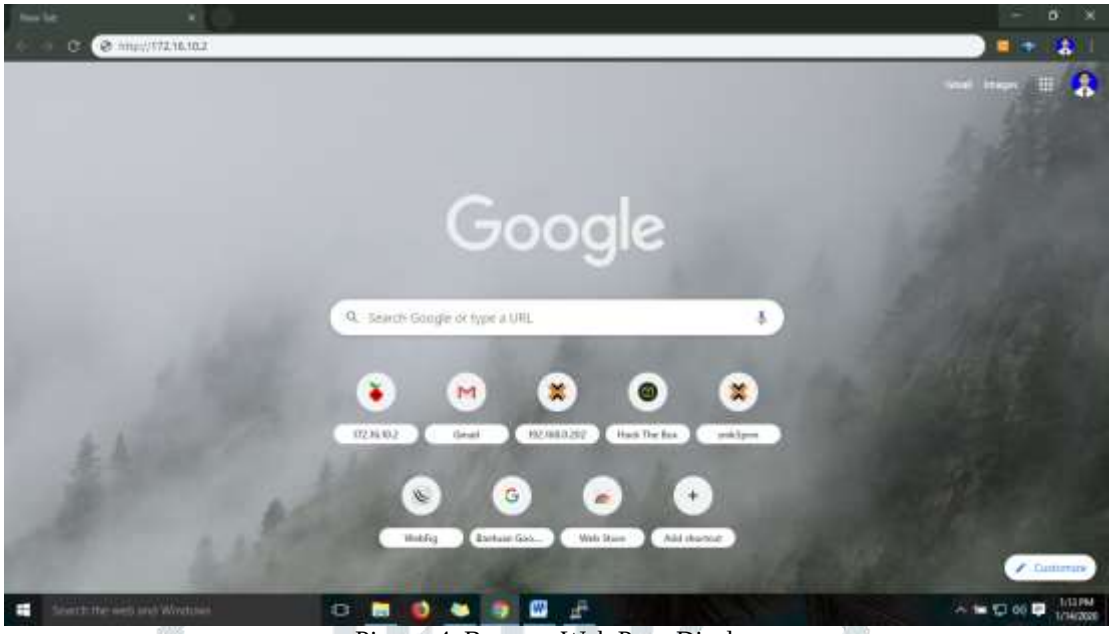
Picture 3. Overall topology

In the topology above can be seen the arrangement as follows:
a. Ether on router 3 to Access point.
b. Wireless on the Router as a receiver from internet sources.
c. The client or user device is connected to the access point wirelessly.
d. There is a firewall to protect the local hotspot network.
e. Pi-hole As Network Security on networks connected using ether 2.
The function of Pi-hole as Network Security is as security on the network and at the same time as an additional firewall that is able to filter data packets that are less secure and suspect.

3.4 Overall Circuit Test

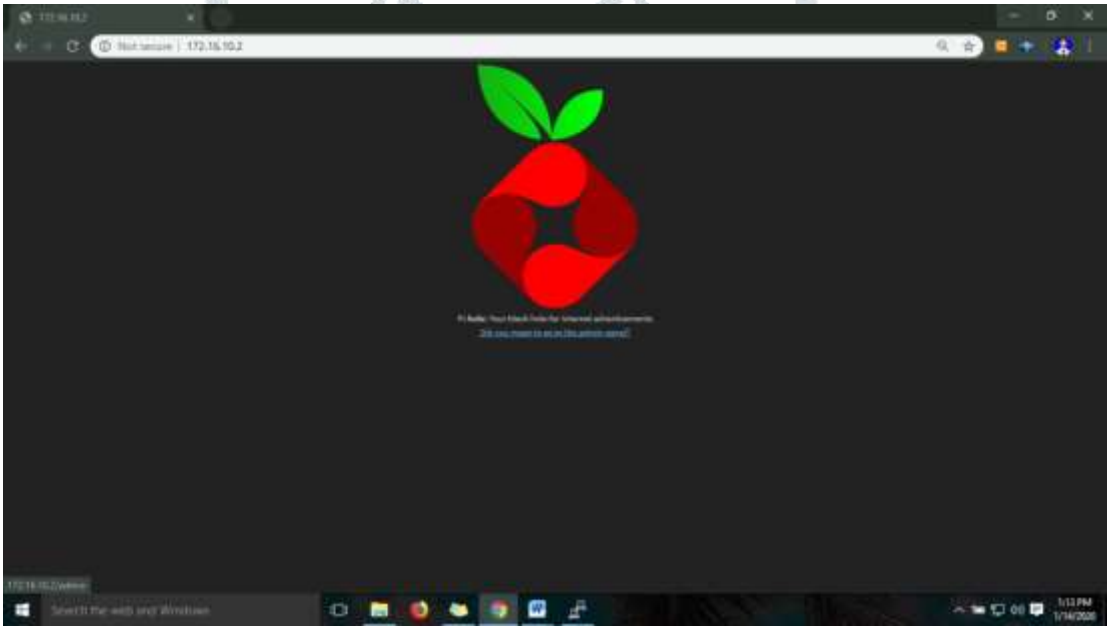
Testing Testing of this system can be done with the following steps:

1. Make sure the device is connected to a paid hotspot, after connecting open the browser and open the http://172.16.10.2 link, a login page will appear. As in Picture 4 below.



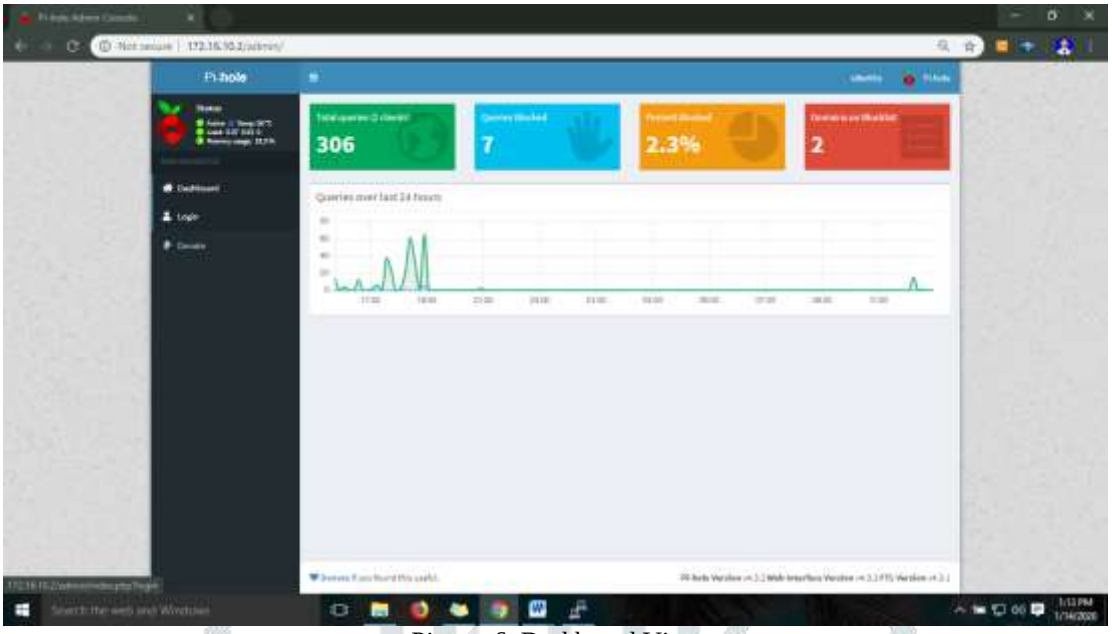
Picture 4. Browser Web Page Display

2. Then a page like this will appear then click the blue text or go to the admin panel. As shown in picture 5 below.



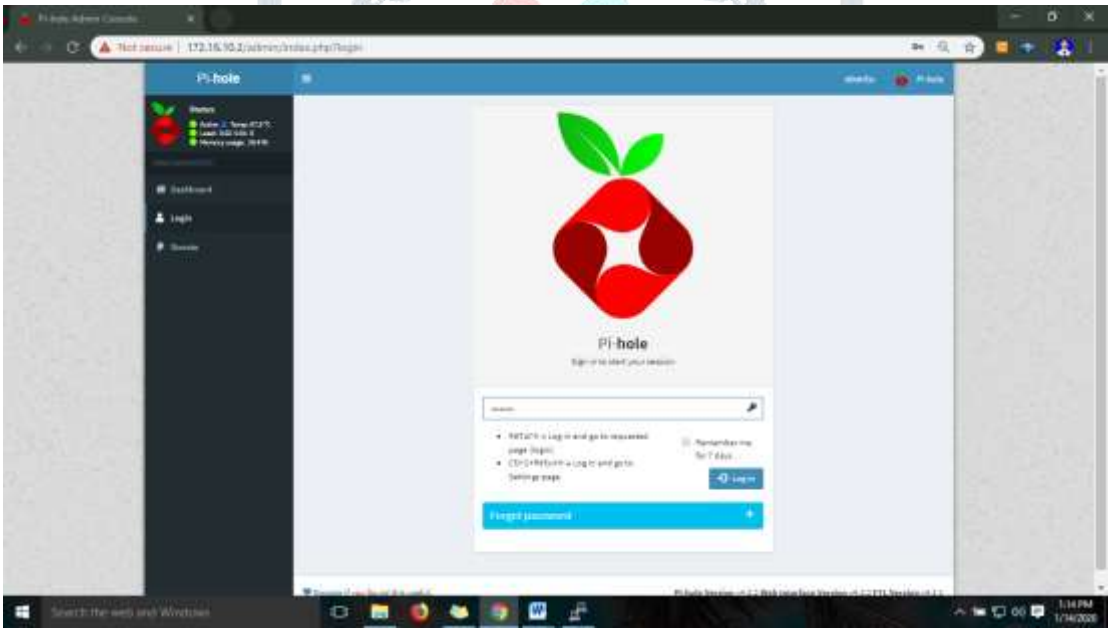
Picture 5. Display the page to the admin panel

3. Next is to go to the pihole admin page where you can only see queries that have been stored in pihole, which can be seen in the following Picture 6.



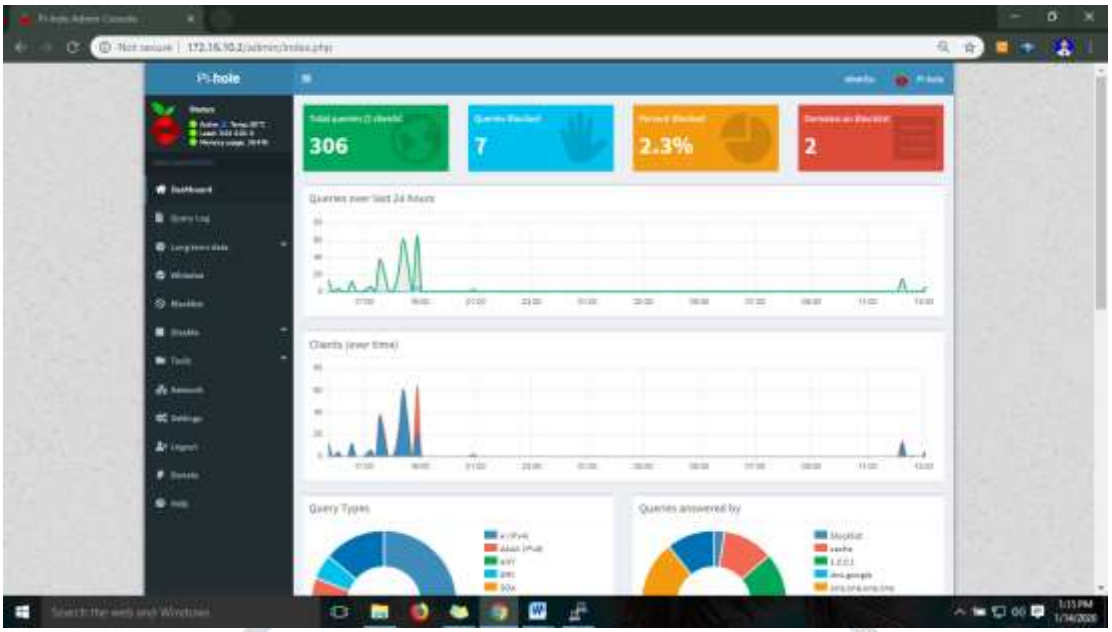
Picture 6. Dashboard View

4. If you want to enter the administrator panel then select login at the bottom of the dashboard as shown in Picture 7 below



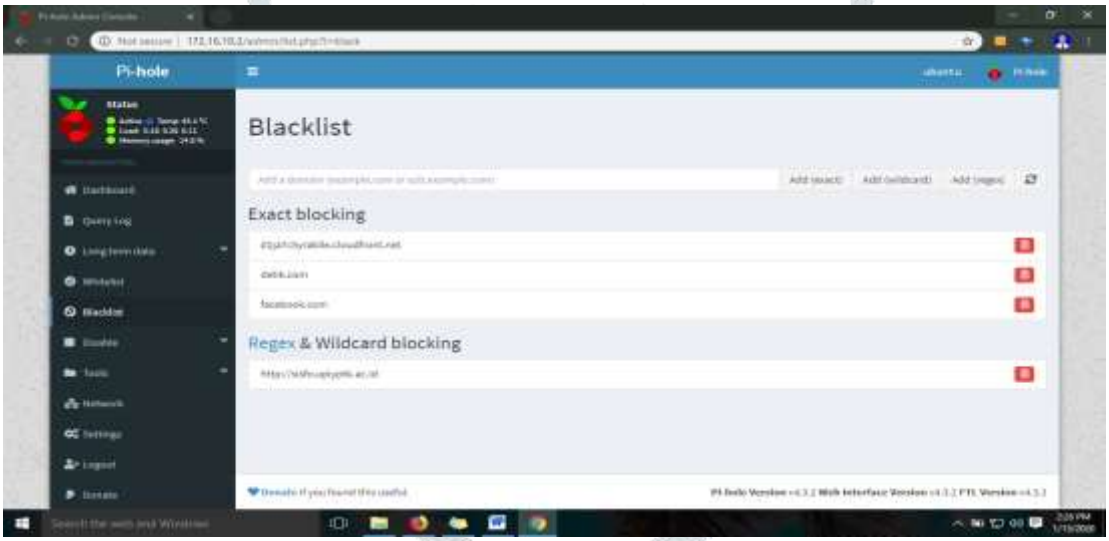
Picture 7. Administrator Panel Display

5. After entering the password, it will enter the administrator dashboard panel page as shown in Picture 8 below.



Picture 8. Administrator Panel Dashboard View

7. Next, block a website or site with the example of campus sisfo http://sisfo.upiyptk.ac.id to test the Pi hole system as shown in Picture 9 below.

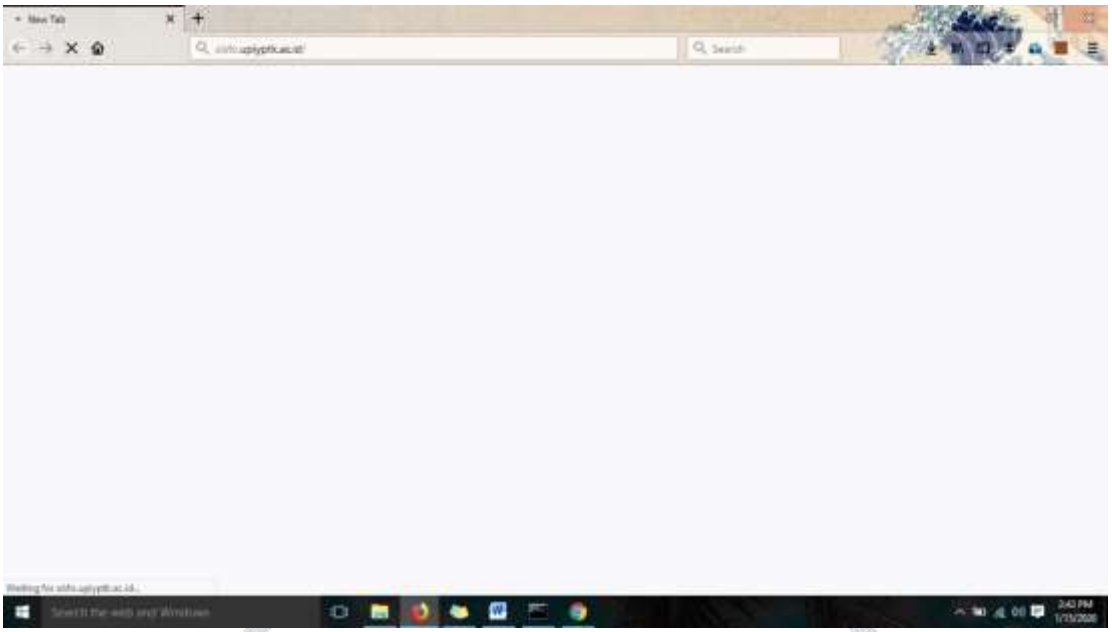


Picture 9. Blacklist Display http://sisfo.upiyptk.ac.id

8. Previously the campus sisfo could be opened properly as shown in the following Picture 10 below

Picture 10. UPI YPTK Information System Display

9. After being entered into the blacklist, the campus information system cannot be opened as shown in the Picture 11 below



Picture 11. The page view does not appear

It can be seen that the campus information system website page cannot be opened because it is included in the blacklist, which means it has been blocked.

3.2 Discussion

One application of network security cannot be separated from the name monitoring system, various kinds of security in an effort to secure information based on local area networks, such as honeynet-based and Intrusion Detection System (IDS)-based, have been proposed. However, IDS-based solutions that use signatures do not appear to be effective.

Through machine learning that is used. It can effectively produce an overall detection accuracy of 90% (journal) by using dns-querry as an information center, therefore through monitoring the PI-Hole firewall also displays dns-querry as a monitoring system but the author adds that the Raspberry is integrated with the mikrotik router making it layered information security applied in the topology presented in the previous chapter (Xuan dau Hoang and Qyunh Chi Nguyen, 2018).

IV. CONCLUSION

Based on the explanations contained in the previous chapters, the following conclusions can be drawn:

1. Filter and block incoming and outgoing content on the network
2. Pi hole is used as an internet condom and as an additional firewall after mikrotik.
3. Pi hole can be applied in industries, schools and government agencies because it is easier to apply.
4. Media Hotspot can help people get internet access to get the information they want
5. This system can foster the interest of writers and readers to conduct entrepreneurship in the field of networking.

REFERENCES

[1] Athailah. Miktorik untuk Pemula 2013. Jakarta.
[2] Conrad Nainggolan dan Syahrizal Dwi Putra. Penggunaan Teknologi Router Mikrotik Dalam Menunjang Jaringan Hotspot Dan Voucher Hotspot Pada Warnet Bnet. Vol.2 No.1 Februari 2018 ISSN : 2597-3673 (Online) ISSN : 2579-5201 (Printed).
[3] Fajar Mochammad Wicaksono dan Hidayat. Mudah BelajarMmikrokontroler Arduino. 2017. Bandung.
[4] Jacob Salmela.Block Ads Network-Wide with A Raspberry Pi-hole. Tahun 2019.
[5] Jasako Mengunakan Codelgniter dan Jquery. 2011 Yogyakarta : Andi
[6] Junaidi Apri. Internet Of Things, Sejarah, Teknologi Dan Penerapannya : Review. ISSN : 2407 – 3911.
[7] Lady Ada. Pi Hole Ad Blocker with Pi Zero W. tahun 2019.
[8] Latipa Herlina Sari dan Aji Sudarsono. Pengembangan Jaringan Local Area Network Menggunakan Sistem Operasi Linux Redhat 9. Vol.9, No.1, Februari 2013.
[9] Nurhayati Ade , Sugiharto Dwi Pantoro. Simulasi Jaringan Vpn Berbasis Mpls Dengan Menggunakan Software Opnet Modular 14.5. Vol VI, No. 11, Nov 2015 , 38-43.
[10] Paul Cobbaut. Linux Fundamental. Version 1.3. tahun 2015
[11] R. Anton Rahaja,Afri Yunianto dan Wisesa Widyanto.Administrasi Sistem Linux. tahun 2001.
[12] Renda dan Herman. Mikrotik Meta Router. 2016.
[13] Sofana Iwan. Membangun Jaringan Komputer. 2013. Bandung.
[14] Sutabri Tata. Analisa Sistem Informasi. 2012. Yogyakarta: Andi.
[15] Thomas Tom. Network Security First-Step. 2005. Yogyakarta: Andi.
[16] Towidjojo Rendra. Mikrotik Kung Fu : Kitab 1. 2016. Jasakom.
[17] Towidjojo Rendra. Mikrotik Kung Fu : Kitab 2. 2016. Jasakom.

[18] Towidjojo Rendra. Mikrotik Kung Fu : Kitab 3. 2016. Jasakom.
[19] Towidjojo Rendra. Mikrotik Kung Fu : Kitab 4. 2016. Jasakom.
[20] Trafena Febi Talika. Jurnal Manfaat Internet Sebagai Media Komunikasi Bagi Remaja Di Desa Air Mangga Kecamatan Laiwui Kabupaten Halmahera Selatan. Volume V. No.1. Tahun 2016.
[21] Triwiyatno Aris. Buku Ajar Sistem KontrolAnalog. 2012. Semarang.
[22] Wahana Komputer. PHP Programing. 2009. Yogyakarta: Andi.
[23] Xuan dau Hoang and Qyunh Chi Nguyen, 2018. Botnet Detection Based On Machine Learning Techniques Using DNS Query Data. *Future Internet* 2018, 10, 43; doi:10.3390/fi10050043.
[24] Yugianto Gin-Gin dan Oscar Rachman. Router . 2017. Bandung.