APPLICATION OF TRANSPARENT DNS, PREVENTION OF USE OF PROXY AND VPN WITH FIREWALL METHOD OF LAYER 7 PROTOCOL MIKROTIK FOR OPTIMIZATION OF NEGATIVE CONTENT FILTERING IN SMAN 27 BANDUNG

Pardan Jamaludin[1], Irfan Dwiguna Sumitra[2]

[1.2] Informatics Engineering Program - Indonesian Computer University
Jl. Dipatiukur 112-114 Bandung
E-mail: pardan14263@email.unikom.ac.id[1], irfan_dwiguna@email.unikom.ac.id[2]

ABSTRACT

Students in schools need technology to assist them in conducting learning activities while in school. Apart from that, there will be a handful of students who use the internet for things that are banned such as opening negative sites. Although the government and ISPs in Indonesia have implemented security to filter out these negative sites, there are still gaps from the security to be easily bypassed. Therefore the author created a network about security to optimize website filtering that has been set by the government and ISPs in Indonesia to build a healthy internet system. This security optimization uses Transparent DNS and Firewall Layer 7 Microtic Protocol. Transparent DNS is a security method where each data packet that passes through the router will be sent to the DNS ISP first. That way, even if the client changes his DNS, the data packet that passes through will be sent to the ISP's DNS first. While the Layer 7 protocol is a pattern search method for data packets in the form of ICMP, TCP, and UDP. The purpose of using Transparent DNS is to prevent students from using external DNS outside the ISP's default DNS so that negative sites can be opened or in other words become unblocked. While the purpose of using the Mikrotik protocol layer 7 firewall is to prevent the use of Proxies and VPNs that are also used to access negative sites.

Keywords : Network Security, Transparent DNS, Layer 7 Protocol, Mikrotik

1. INTRODUCTION

Internet Service Providers (ISPs) or internet service providers in Indonesia must block sites that contain negative elements. This is in accordance with KOMINFO Ministerial Regulation of the Republic of Indonesia Number 19 Year 2014 Article 8 Paragraph (1). With the existence of this regulation, it is expected to be able to distance the public from the negative impact of the internet.

From the results of the research interviews that the authors did at 27 Public High Schools in Bandung, there had been a block on the sites found on TRUST + Positive through the security of the ISP they used, namely Indihome. However, there is no additional security that causes a gap to pass through positive internet security imposed by the ISP. Therefore, the author has the idea to do additional network security to optimize the blocking of negative sites.

In preventing the above, a mechanism is created in an effort to maintain network security or commonly called Firewall. A firewall is a system that allows unsafe network traffic. Usually, firewalls are implemented in agatewaybetween local networks and other networks. Firewall is also usually used to control access to anyone who has access to networks from outside parties.

The security that the author will apply there is from the side of DNS, proxy, and also VPN. Security from the DNS side uses Transparent DNS, where each data packet that passes through the router will be sent to the DNS ISP first. That way, even if the client changes his DNS, the data packet that passes through will be sent to the ISP's DNS first. It's like we force the client to enter the ISP's DNS.

Apart from DNS, another loophole for bypass positive internetis to use a proxy and also a VPN. Therefore, the author will also try to apply the blocking of using Proxy and VPN by using the L7 Protocol firewall from Mikrotik to preventfrom clients accessing negative internet content.

According to the agreement with the headmaster and staff ITthere, they want to be able to see what access is done by students who use the internet at 27 Public High School Bandung. So, if there are still those who are seen using the internet for things that are not fair, they can be followed up with punishments such as dismissal of internet access for a specified time or can be reprimanded by the parties concerned.

Based on the background of the problem above, the author intends to take the topic of this thesis entitled "Application of Transparent DNS, Prevention of Use of Proxy and VPN with Firewall Method Layer 7Microtic Protocol for Optimizing

Filtering Negative Contentand Implementation in SMAN 27 Bandung"

The purpose of this research is to improve network security from the client side to be more optimal. While the purpose of this study was as follows:

a. Applying Transparent DNS so that clients continue to use the DNS ISP though replacing the settings
b. Blocking the websites of the service provider Proxy and VPN Service uses L7 Protocol Mikrotik
c. Applying disconnection Internet access to the client for 1 minute if they try to use internet to open negative sites

2. RESEARCH CONTENT

2.1 Literature Review

following is the theory used as a reference in this study.

2.1.1 Computer Networks Computer

networks are two or more separate systems, through communication media to communicate data from one source with other sources to share resources.

While computer networks according to Harry Prihanto are a group of computers that number more than one or many separate ones, but are interconnected in doing their tasks or connected to each other. [1]

Based on the definition, it can be concluded that computer networks are a separate system for communication in order to exchange information.

2.1.2 Firewall

Firewall is a device whose task is to check data packets that can enter or exit a network. In other words, firewallsa playrole in protecting the network from attacks originating from non-local networks oroutside networks. [2] A

firewall implements packet filtering and also a security function that is used to manage data flow from, to, and through a router. For example, a firewall is used to protect local networks (LAN) from possible attacks that come from the Internet. In addition to protecting the network, a firewall is also used to protect the user's computer or host (host firewall). [2]

2.1.3 DNS (Domain Name System)

Each network interface connected to the TCP / IP network is identified through an IP address. A name (hotname) can also be given to any device that has an IP address such as: server, router, terminal, and so on. Network software does not require a name to connect. However, we as network orusers network need this because it is easier to remember and type than the IP address that the computer requires. Naming each computer that is connected to each other. On the Internet, each device is given an informative name. By looking at the name of a device, we can at least imagine where the device is and service whatis provided. The form of the site domain used on the Internet is similar to the IP Address, which consists of several segments. Each segment is a name or abbreviation that provides information. [3]

2.1.4 Proxy

proxy acts as a gateway to this Internet world for each client computer. Proxies are not visible to the client computer, in other words, a user who interacts with the Internet using a proxy will not know that a proxy is handling the request. The web that accepts requests from the proxy will interpret those requests as if the request came directly from the client computer, not from a proxy. [4]

2.1.5 VPN (Virtual Private Network)

Virtual Private Network (VPN) is a communication technology that makes it possible to connect to a public network and use it to join a local network. In this way, the same rights and settings will be obtained as well as being in a network itself, even though it actually uses a public network. [5]

2.1.6 Types of Negative Content

Contentcontent is now scattered on the internet. The internet does not only belong to a handful of people but ours is what happens if the content of negative content is spread on the internet but we cannot act because we have no power. Negative content that is intended in this study is like pornography, online gambling, and so on. The list of negative contents is found in the Trust + Positive Kominfo site database, namely: https://trustpositif.kominfo.go.id/

2.1.7 Mikrotik

Mikrotik is an operating system and also software that can be used to make computers become router networks reliable, includes various features made fornetworks wireless and IP networks. Mikrotik was created to be easy to use and very good for the purposes of controlling computer networks such as designing and building a small-scale computer network system to a complex or large even though [6]

2.2 Research Methods

Research Methods is a process used to solve a logical problem, in where do you need data to support the implementation of a study. The research method used is descriptive analysis method which has two stages, namely data collection and network development.

2.2.1 Data Collection Methods The data

collection methods used in writing this essay are as follows.

a. Literature Studies

Study books, articles and papers related to the topic of the final assignment.

b. System Design The

design carried out includes designing a network topology, preparing the needs of the device, and installing an operating system and applications that are used to optimize so that it can run well on the system.

c. Implementation

Implementation is done in the form of system implementation and configuration of Transparent DNS, Blocking Proxy and VPN to optimize filtering negative contentimposed by ISP

d. Testing

Testing is done by using theDNS default provided by the ISP, using External DNS, and using Proxy and VPN

e. Analysis and Conclusions

After testing the DNS, Proxy, and VPN, conclusions can be drawn.

2.2.2 Network Development Method

Method used in this study is the NDLC model. Network Development Life Cycle (NDLC) is a model that relies on the model of the network lifecycle with the concept NDLC ie, Needs Analysis(Analysis),Design(Design),Simulation(Sim ulationPrototype),Implementation(Implementation), Monitoringand Management.If the implementation of network technology is implemented effectively, it will provide an information system that will fulfill the objectives. The following are the stages of the NDLC. [7]

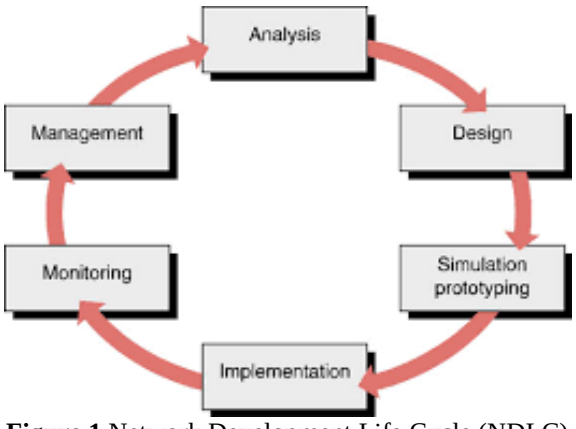

Figure 1 Network Development Life Cycle (NDLC)

a. Analysis

This stage requires an analysis of the problems that arise, analysis of user desires and hardware requirements to be used and analysis of network topologies that currently exist.

b. Design (Design)

Design or design can be in the form of topology structure, data access design,design layout cablingand so on that will provide a clear picture of the project to be built.

c. Simulation (Simulation Prototype)

In the simulation phase the author builds a simple network on the project that will be built using all the tools that will be used in the application.

d. Implementation (Implementatiton)

In the implementation phase the author will configure a LAN network and also Wireless. This implementation begins with the basic setting of

e. Monitoring

The surveillance model of the NDLC network system categorizes the testing process at thestage monitoring. This is because the supervision of the system has been built or developed. The testing process is to guarantee whether the system that is built or developed can run and in accordance with the wishes. At this stage the author monitors the user using Mikrotik. Steps are carried out with the aim of ensuring the network runs well.

f. Management

Next is management or management. This phase includes the activities and maintenance of all systems that have been built. Thisphase management will be carried out after the system is running properly on the network that has been built. In thestage the management writer will take several management steps so that the system that has been built can run in accordance with the expected.

2.3 Results and Discussion

following is a discussion of the research that will be built along with the results.

2.3.1 Analysis of Systems

Analysis is an action taken to find out more details about the object to be studied. This section will describe the needs analysis, network design analysis and system configuration. The initial stage is to analyze the basic needs of the configuration that will be built. At present, positive internet security at Indonesian ISPs is only done from their DNS side. If the user changes DNS settings using DNS other than those provided by the ISP, then a positive internet security will bebypassed. In addition, there are also other avenues such as using a proxy and VPN. administrators Networkat SMAN 27 Bandung have not been able to limit the use of DNS External, proxy, and also VPNs in the SMAN 27 Bandung environment

2.3.2 Network Architecture

Here is a network architecture that currently runs in Public High School 27 Bandung.

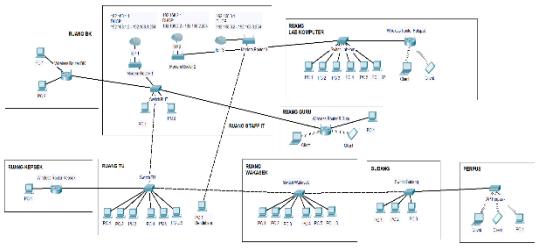

Figure 2 Current Network Architecture

Then the network architecture for this implementation is how a Routerboard Microt can prevent the opening of sites with negative content and has been configured to stop the internet connection of users who keep trying to open the site according to the specified time. The following is an overview of network architecture after implementation.

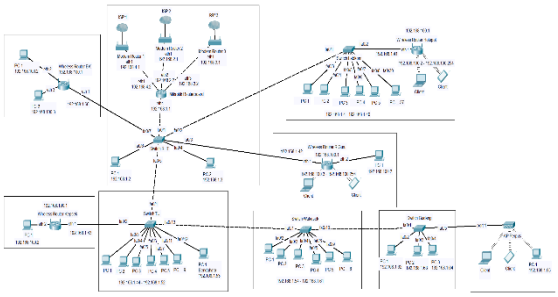

Figure 3 Network Architecture After Implementation

In addition, there is an IP address allocation used at SMAN 27 Bandung. Public IP used from ISP for SMAN 27 Bandung is dynamic and IP for local network is static. The following is the IP address allocation at SMAN 27 Bandung.

Table 1 Allocation of IP Address

Device	IP Address	Gateway	Interface
Wireless Router ISP1	(IP Dynamic	)	ether1
	192.168.4.1/24	-	ether2
ISP Wireless Router 2	(IP Dynamic)	(IP Dynamic)	ether1
	192.168.2.1/24	-	ether2
ISP Wireless Router 3	(IP Dynamic)	(IP Dynamic)	ether1
	192.168.3.1/24	-	ether2
Mikrotik Routerboard	192.168.4.2/24	192.168.4.1	ether1
	192.168.2.2/24	192.168.2.1	ether2
	192.168.3.2/24	192.168.3.1	ether3
	192.168 .1.1 / 24	-	ether4Microtic

2.3.3Configuration

The routerboard configuration is the stage where settings for some parameters are carried out on the routerboard so that it can perform positive internet optimization. The parameters that will be configured on the proxy routerboard are as follows:

a. IP Address
b. configuration stage DNS
c. configurationRoute
d. stage IP configuration phaseIP configuration stage NAT Address
e. Phase check connection
f. NAT firewall configuration stage for Transparent DNS
g. Phase configuration firewall Layer7 Protocols for
h. blocking proxy and VPN

The above configuration stages are carried out in stages so that if something goes wrong it can be easy to fix it. The following is a picture of the Mikrotik configuration in stages.

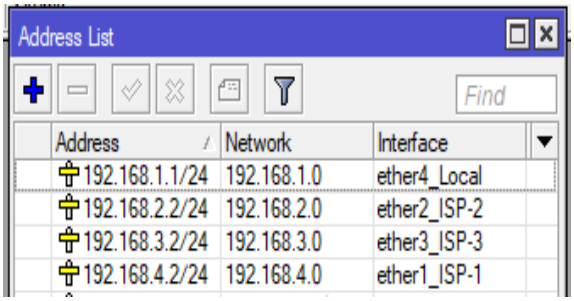

Figure 4 IP Address Configuration

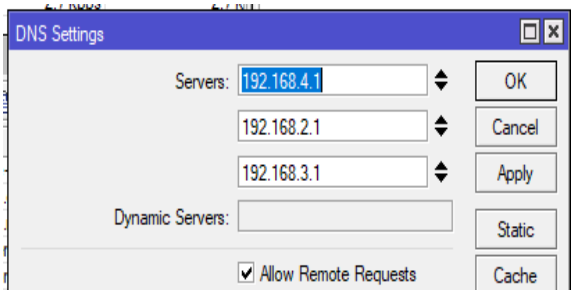

Figure 5 DNS Configuration

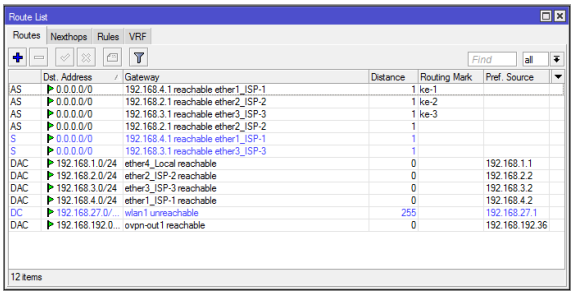

Figure 6 IP Route Configuration

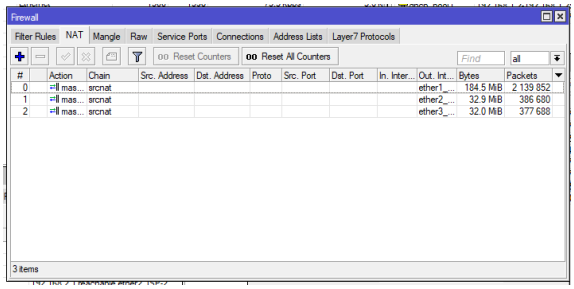

Figure 7 NAT Firewall IP Configuration

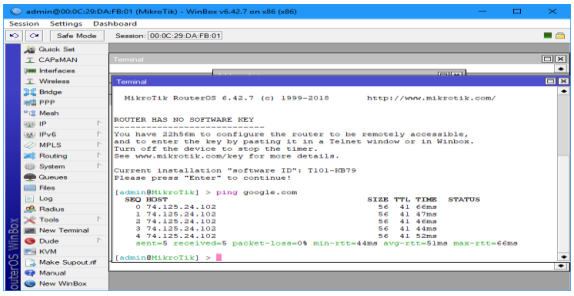

Figure 8 Check Connection

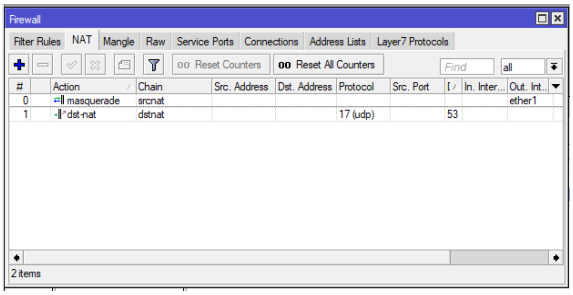

Figure 9 Transparent DNS

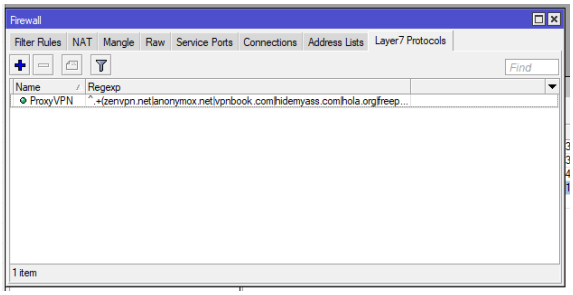

Figure 10 ConfigurationL7 Protocol

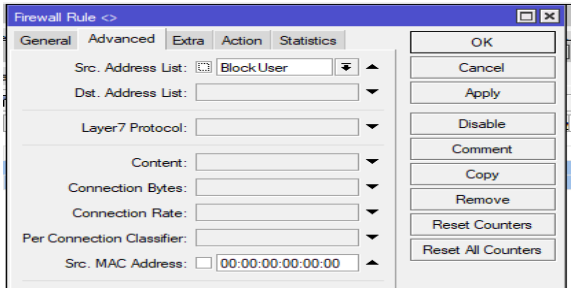

Figure 11 ConfigurationBlock User Configuration

2.3.4 Testing Scenario

Testing scenario here is used as a reference when testing the configuration results, the testing scenario that will be carried out is made into several test scenarios related to the configuration implemented. The testing scenario that will be carried out focuses on the system configuration that has been done in Mikrotik and the commands that will be used in the media.

Based on these parameters, five main test scenarios will be made that are implemented. The scenarios tested are as follows.

a. Accessing negative sites with DNS:
   - Using default DNS without configuration Transparent DNS
   - Using external DNS without configuration Transparent DNS
   - Using default DNS with Transparent DNS configuration
   - Using external DNS with configuration Transparent DNS

b. Testing proxy usage:
   - Without using L7 Protocols Mikrotik
   - configuration Using L7 Protocols Mikrotik configuration

c. Test VPN usage:
   - Without using L7 Protocols Mikrotik
   - configuration Using L7 Protocols Mikrotik configuration

2.3.5 Testing Results

a. DNS Testing The

author tries to change the DNS settings on thedevice client using Cloudflare's DNS ie.

Primary DNS : 1.1.1.1
Secondary DNS : 1.0.0.1

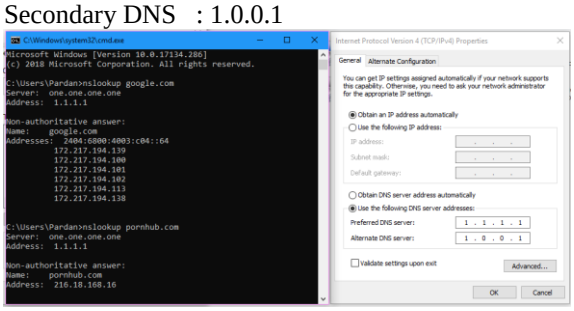

Figure 12 Changing DNS Settings Without Transparent DNS

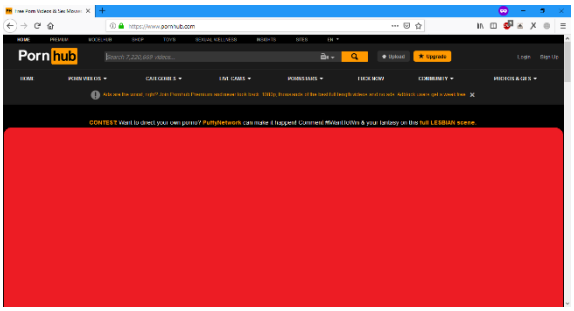

Figure 13 Opening Negative Sites Using DNS Cloudflare

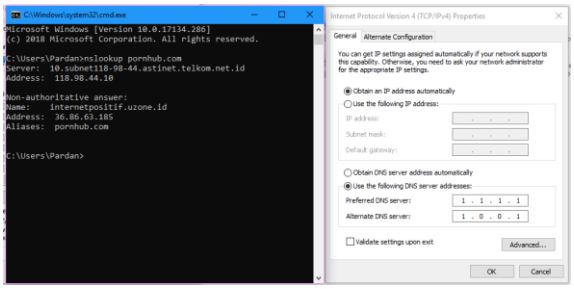

Figure 14 Changing DNS Settings With Transparent DNS

Figure 15 Opening Negative Sites Using Cloudflare DNS Transparent DNS

Conclusions from testing in the DNS stage can be seen in Table 2 below.

Table 2 Conclusions DNS TestingDNS

Types ofTests	Contesting Sites Negative
DNS Without Transparent DNS	Blocked
External DNS (Cloudflare) Without Transparent DNS	Not Blocked
Default DNS Transparent DNS	Blocked
External DNS (Cloudflare) Transparent DNS	Blocked

b. Proxy Testing

At this stage a proxy use test will be conducted to unblock negative content sites imposed by ISPs. The testing that the author will do is divided into two stages, namely the use of a proxy without the configuration of the L7 Protocols Mikrotikand with theconfiguration firewallL7 Protocolsfirewall Mikrotik.

The test in this step will be done using the Web Proxy from https://whoer.net/webproxy

Figure 16 Whoer.net Web Proxy

Although it has implemented aconfiguration system Transparent DNS, negative sites can still be accessed by clients. One of them is using a proxy or web proxy such as whoer.net. The following is testing using Whoer.net without activatingconfiguration layer 7 protocols firewall to access sites with negative content.

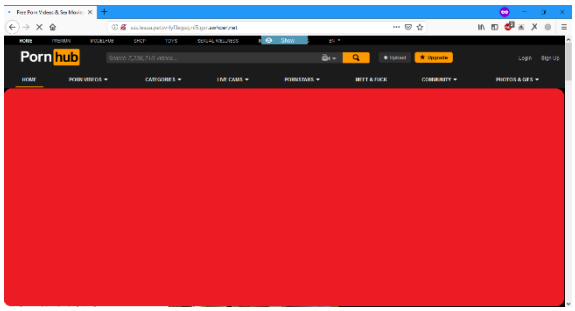

Figure 17 Accessing Negative Sites Using a Web Proxy Without Firewall L7 Protocols Microtics

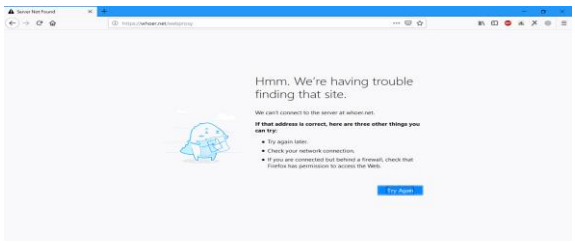

Figure 18 Accessing Negative Sites Using Web Proxies With Firewall L7 Protocols Microtics The

conclusion of this Proxy testing phase can be seen in Table 3 below.

Table 3 Conclusion Proxy TestingProxy

Types ofTesting	Information
Using the Web Proxy whoer.net without configuration Layer 7 Protocols Mikrotik	Not Blocked
Using Web Proxy Whoer.net with Layer 7 Protocols Microtic	Successfully Blocked

c. VPN Testing

At this testing stage, the author will use ProtonVPN to access negative sites.

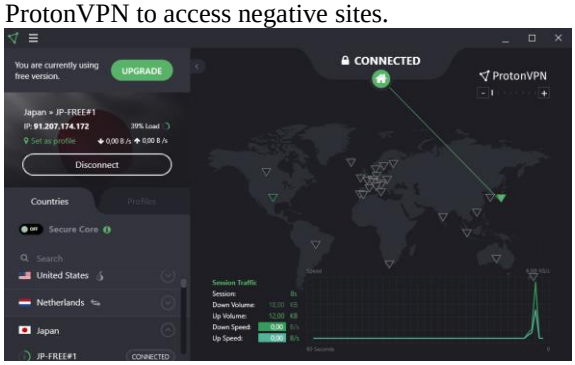

Figure 19 ProtonVPN Successfully Connected Without Firewall L7 Microtic Protocols

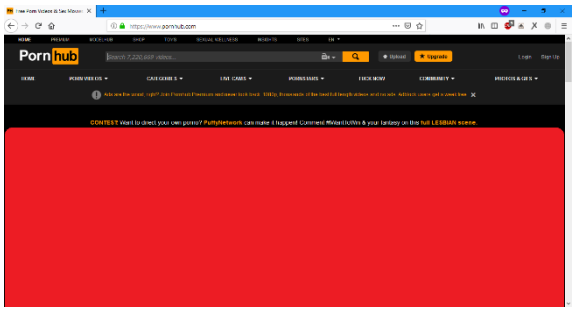

Figure 20 Open Negative Content Site Using ProtonVPN

Furthermore, as before, in this test the author will use ProtonVPN to access sites with negative content. But by activatingsecurity Layer 7 firewall the

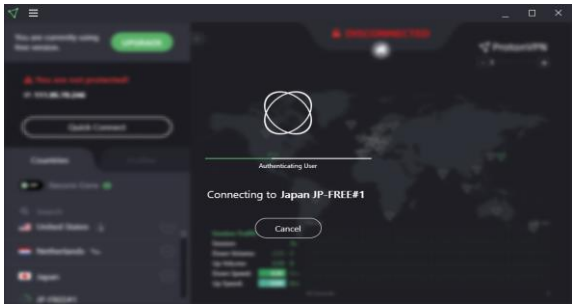

Figure 21 ProtonVPN Not Be Connected After the Enable Firewall Mikrotik L7 Protocols

VPN conclusion of the testing phase can be seen in Table 4 below.

Table 4 Conclusions on VPN TestingVPN

Types ofTesting	Information
Using ProtonVPN without configuration Layer 7 Protocols	Not Blocked
Microtics AreUsing ProtonVPN with Layer 7 Protocols Microtics	Successfully Blocked

3. CLOSING

3.1 Conclusions

After doing design analysis and testing, conclusions can be drawn as follows:

a. Transparent DNS makes client use theDNS default provided by the ISP so that internet usage will be more secure
b. Layer 7 Protocol is one method in blocking sites, applications, and file extensions.
c. Through afirewall,an addresshost of thethat is entered will be blocked, so that they will not be able to connect with address the

3.2 Advice

Below is a description also suggestions that might be taken into consideration in the development of penetilian this, such as:

a. Can be developed to cultivate the effectiveness of the use of Layer 7 Protocol on a larger internet network
b. Increase the list of proxy applications and also VPN so that internet network security is more optimal
c. Prevent the use of DNS through other channels such as DNS Over HTPS and TLS

REFERENCES

[1] Prihanto, Harry, Building a Computer Network: Knowing Hardware and Network topology , Bandung, 2016.
[2] I. Riadi, Block Site with Layer 7 Microtic and Web Proxy, Jakarta, 2015.
[3] Daryanto, Computer Engineering Network, Bandung: Alfabeta, 2010.
[4] Towidjojo, Rendra, Mikrotik Kungfu Kitab 3, Jakarta: Jasakom, 2013.
[5] Irawan Afrianto, Eko Budi Setiawan, "VIRTUAL PRIVATE NETWORK (VPN) STUDY AS SIS TEM DATA SAFETY ON COMPUTER NETWORK (Case Study of UNIKOM Computer Network), " UNIKOM Scientific Magazine, vol. 12, p. 1, 2014.
[6] Towidjojo, Mikrotik Kungfu Volume 1, Jakarta: Jasakom, 2015.
[7] Herlambang, M.Linto, Building Sharing Internet Connection at Mikrotik, Yogyakarta: Andi, 2015.