Jurnal Mantik, 5 (3) (2021) 1584-1590

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Network Security to Protect Negative Web: A Case Study of The Government of Aceh

Syafrinal[1], Abdus Salam[2]

[1] STMIK Indonesia Banda Aceh, JL. Teuku Nyak Arif, Simpang Mesra, Jeulingke, Syiah Kuala, Banda Aceh City, Aceh Province, Indonesia.
[2] AMIK Indonesia, JL. Teuku Nyak Arif, Simpang Mesra, Jeulingke, Syiah Kuala, Banda Aceh City, Aceh Province, Indonesia.

E-mail: syafrinal@stmikiba.ac.id

A R T I C L E I N F O

Article history:

Received: August 10, 20201
Revised: September 01, 20201
Accepted: October 15, 20201

Keywords:

Security;
Network;
Protection;
Negative Web.

A B S T R A C T

The specific objectives of the research include evaluating the extent to which information governance management has been carried out at the Aceh Communications, Information and Encryption Service, and negative web protection that is accessed through the aceh government network in all OPDs and districts/cities throughout Aceh. This research will use 4 (four) stages of information system security audit including; audit planning, preparation, implementation, and reporting. Information system security audit. There are several conclusions drawn based on the discussion on the results of the analysis. The conclusions drawn from this study are 1) Based on the results obtained from this practical work course project, almost all HTTP and HTTPS protocol websites can be blocked using the filtering techniques available on MikroTik, 2) Using a VPN is almost impossible to block using MikroTik because the settings proxy to block VPN is very complicated, and 3) MikroTik device is able to block almost all websites using Layer7 and mangle and can't turn off VPN traffic.

1. Introduction

Based on Aceh Governor Regulation Number 119 of 2016 that the Aceh Communication, Information and Encryption Service (Diskominfo and Aceh Sandi) has the authority to manage technology and information assets in the Aceh Government. As an institution that manages information systems in the Aceh Government, Diskominfo and Sandi Aceh have utilized information technology and have implemented services in carrying out good governance efforts for the Aceh Government's information system security to build reliable and reliable services in managing data. Centralized center. Along with the rapid and sophisticated development of the world of technology, the internet is a communication network that uses electronic media (Fathurrahmad, & Yusuf, 2019), which are connected to each other using the global standard TCP/IP system as a packet exchange protocol (Sarno, 2009; Fathurrahmad et al. al, 2019). The internet must be used wisely (Pinariya & Lemona, 2019) to prevent users from accessing the internet negatively, namely pornography, gambling, SARA, piracy, hoaxes, and others (Suroso, 2019; Hwian, 2017). The consequences of accessing websites are negative and affect the mentality of a human being (Haniza, 2019). The Ministry of Communication and Informatics (Kemkominfo) is a Ministry within the Government of Indonesia in charge of communications and informatics affairs. The main role of the Ministry of Communication and Information is to monitor all websites that will be filtered using TRUST+ filtering. Website blocking must be done carefully so that unwanted things do not happen.

Some websites have domains and have HTTP and HTTPS protocols. HTTP protocol is a protocol that is not commonly used because it can cause data leakage. Whereas HTTPS already uses SSL encryption and

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

leaks are easier to prevent. Blocking HTTP websites is easier than HTTPS. Based on these problems, researchers are interested in conducting further research related to network security by using HTTP and HTTPS website filtering using MikroTik (MikroTik ID, 2020). For HTTP you can use a web proxy, while HTTPS uses Layer 7 to block websites. After that it blocks VPN traffic as website tunneling (MikroTik ID, 2020). The specific objectives of this research are:

a. Evaluate the extent to which security management has been carried out at the Aceh Communications, Information and Encryption Office.
b. Designing a model regarding website filtering for negative web protection network security.

The related research conducted by Sulaiman (2016) conducted a simulation implementation trial using Cisco packet tracer 6.2, an analysis was carried out on each type of switch port security to determine its reliability, usability, and utilization in the field. Meanwhile, Muzakir and Ulfa (2019), simulated a network security system using Wireshark on every packet sent that could not be read (blocked) both on the HTTP and HTTPS protocols. The performance of the tools in a proxy router does not guarantee good security, the effectiveness of security depends on the administrator's ability to configure the security. Another case was done by Holik et al (2020), making a defined network concept for software applied to an industrial network. In this study, the Industrial Network Protection System (INPS) is designed and implemented and focuses on developing the decision function of the Artificial Intelligence (AI) module. As a result, an artificial neural network model was created, which was used for network traffic evaluation in the AI module, developed and tested comprehensively.

Previous research conducted by Muklas, Supendar, and Sulistianto (2020), where the firewall filtering system and web proxy filter negative sites. The results of the study found that the proxy web proxy was able to block sites both URLs, keywords, and time settings for using social network access. In this study, MikroTik could not block all negative content on the internet. Noviansyah. and Saiyar (2020) also conducted research on the application of a web proxy using a proxy router to block social media sites and streaming sites to support user work activities. After the implementation of a web proxy, users cannot access sites that are not suitable for work and learning, and only users who can pass the authentication process can access the wireless network. Based on previous research, limiting the use of internet access can minimize the occurrence of data leakage and negative behavior from users.

2. Method

2.1 Research Objects and Paths

Based on the results of the literature study, conclusions are drawn from various similar studies that have been carried out to determine the best system flow and in accordance with the research case study. The network topology design used remains the same model as the initial network topology design. Changes made to convert MikroTik into an Intrusion Detection System (IDS) are the use of firewalls and mail. The Intrusion Detection System workflow begins with the detection of data packets that are considered dangerous by the firewall, along with the sequence of actions taken by the firewall. The research flow is carried out as shown in Figure 1 Research Flowchart.

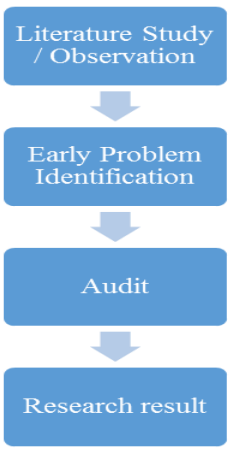


Fig 1. Research Flowchart

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

2.2 Research Sites and Equipment Needs

The research was conducted in the Information and Communication Technology Division of the Aceh Communications, Information and Encryption Service, as well as tools and materials to support this research in the form of hardware used is a Lenovo laptop with an Intel® Core (TM) i3-3230M @ 2.60 Ghz processor, and 6.00 RAM. GB. The operating system used is Windows 7 PC. The software to support this activity is Winbox and Google Chrome.

2.3 Steps and Stages of Information System Security Audit

The steps and stages of the work process consist of several important stages, starting with connecting the proxy router and blocking websites using web proxies and layer 7 and disabling VPN (Virtual Private Network) traffic.

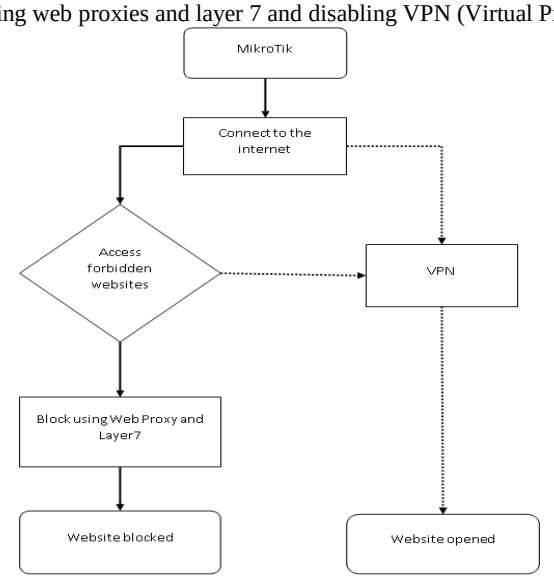


Fig 2. Flow Method and Work Process

3. Results and Analysis

3.1 Data

Web page data that has been filtered is 296,619 originating from the TRUST+ domain belonging to the Ministry of Communications and Informatics and Internet Syariah, totaling more than 2.6 million blacklisted websites. The negative site category consists of several categories, namely:

a. Pornography
b. Fraud
c. Gambling
d. Malware
e. Radicalism/Terrorism
f. SARA/Hate
g. Child Porn
h. Violence
i. Copyright infringement
j. Etc.

3.2 Work Steps

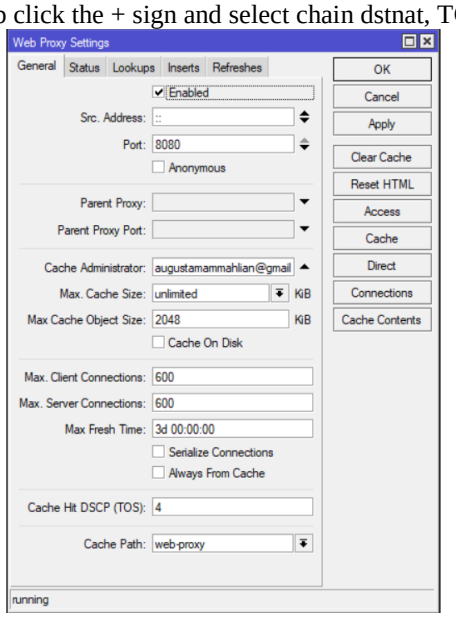
Before filtering the website, all tools and materials must be prepared to work on a project to block domains from negative websites which consists of two protocols namely HTTP and HTTPS. The steps taken are:

a. Connecting the Device
b. HTTP Website Filtering
c. HTTPS Website Filtering
d. Closing VPN Access

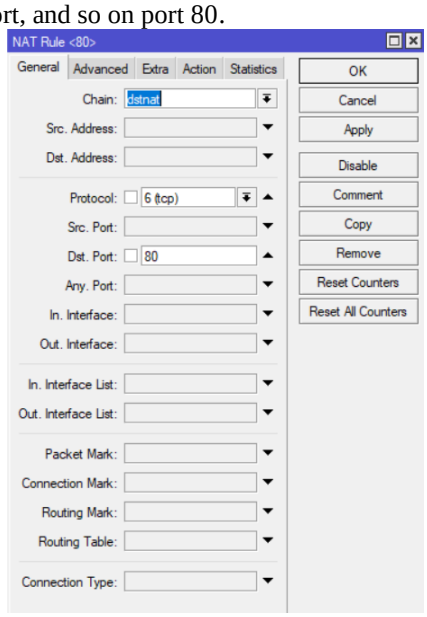
Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

3.3 Filtering Website HTTP

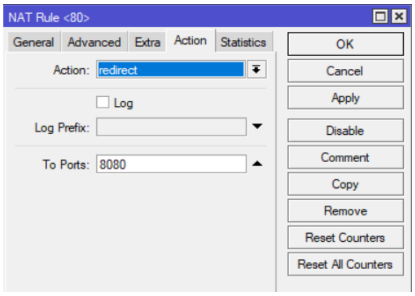
After the Mikrotik device is connected to the internet, then open IP Web Proxy and then tick Enable. Terms of activating Web Proxy must first activate Transparent Proxy by clicking IP → Firewall and in the NAT tab click the + sign and select chain dstnat, TCP port, and so on port 80.



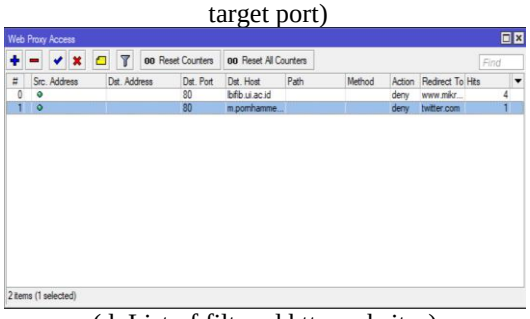
(a. Web Proxy)



(b. Command to enable Transparent Proxy target port)



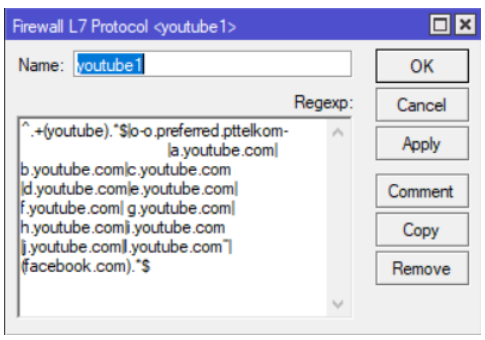
(c. Command to activate Transparent Proxy redirect to website)

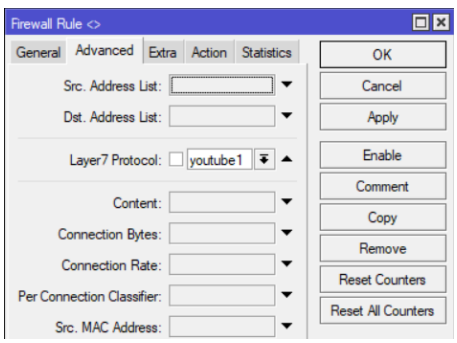


(d. List of filtered http websites)

3.4 Filtering Website HTTPS

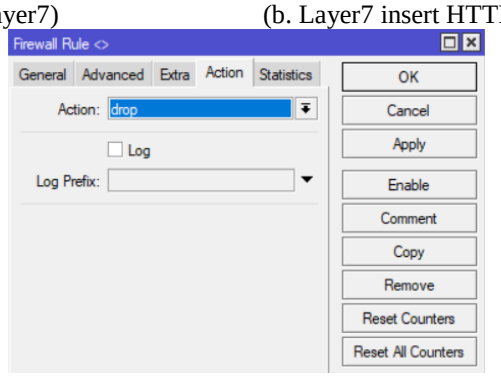
To cover the weakness of the web proxy as a substitute for filtering using Layer7. Enter the IP menu → Firewall and click the Layer7 Protocol tab. Enter the filtered URL address by including the website name and Regexp.





Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

(a. Rule Layer7) (b. Layer7 insert HTTPS filtering command)



(c. HTTPS filtering command blocks websites)

3.5 Results and Discussion

In this study, the results obtained through access to websites that are filtered using a web proxy and layer7 are:

a. Using a Web proxy

The results of Figure 4.17 can be seen that the HTTP website has been blocked using a web proxy without redirecting to another site.

Fig 3. HTTP website has been blocked

The results from Figure 3 can be seen that the HTTP website has been blocked using a web proxy and can redirect to all other sites.

b. Using Layer 7

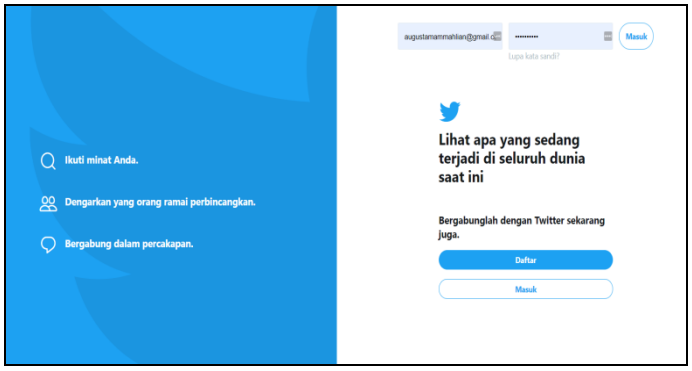


Fig 4. HTTP website has been redirected to another site

Based on the results above, we can see that access to the prohibited website will be redirected to another website that contains this page cannot be accessed. Filtering using a Web Proxy is a bit more complicated because you have to activate the transparent proxy first. For HTTPS websites such as thepiratebay.org, it is almost impossible to filter using a Web Proxy because the site from the domain is encrypted with SSL. In general, HTTP protocol websites are marked as insecure in some browsers.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

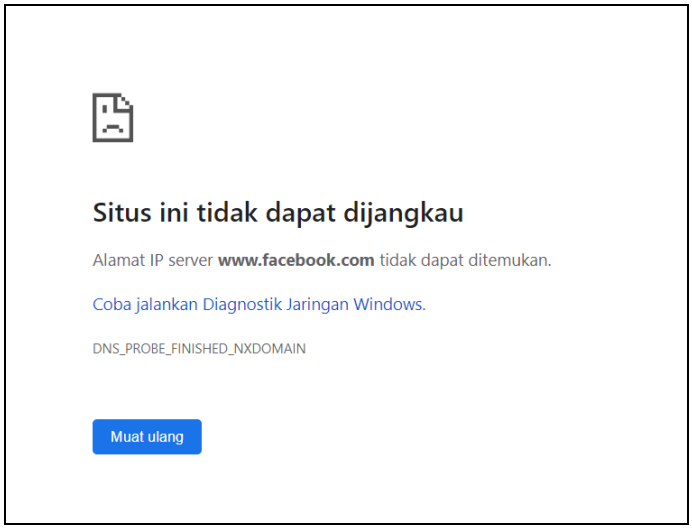


Fig 5. HTTPS website has been blocked

Based on the results above, it can be seen that website access that has been filtered using Layer7 automatically refuses to connect. Filtering using Layer7 is more practical by including Regexp. All websites today use HTTPS to protect data from leaks. Almost all browsers already have a lock symbol when accessing the website.

3.6 Discussion

Maintaining data security and internet use in cyberspace can not only be done by administrators and human resource management in an agency. Even though education and direction have been carried out, there needs to be synergy and intensive collaboration with stakeholders, namely the government to provide internet literacy to employees so that they can fortify themselves and surf the internet safely. Filter techniques in MikroTik can be used as an alternative in preventing negative websites from being crawled by employees. Some studies have applied various techniques and the use of artificial intelligence in limiting the use of negative web, some are expensive. However, this study provides a solution only for facilities that are already available at the Aceh Government agencies so that MikroTik management can be used very well in managing negative content.

4. Conclusion

There are several conclusions drawn based on the discussion on the results of the analysis. The conclusions drawn from this Practical Work Lecture are as follows:

a. Based on the results obtained from this practical work course project, almost all HTTP and HTTPS protocol websites can be blocked using the filtering technique in MikroTik.
b. Using a VPN is almost impossible to block using a proxy because setting up a proxy to block a VPN is very complicated.
c. MikroTik device is able to block almost all websites using Layer7 and mangle and can't turn off VPN traffic.

5. Reference

[1] Bansal, K., Masurekar, U., Srinivasan, A., Shah, S. and Maskalik, S., Nicira Inc, 2019. Method and apparatus for distributing firewall rules. U.S. Patent 10,264,021.
[2] Ceragioli, L., Degano, P. and Galletta, L., 2019. Checking the Expressivity of Firewall Languages. In The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy (pp. 86-100). Springer, Cham.
[3] Dewi, S., 2016. Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. Yustisia Jurnal Hukum, 5(1), pp.35-53.
[4] Dwiyatno, S., 2020. Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 7(2), pp.108-115.

[5] Fathurrahmad, F. and Yusuf, S., 2019. Implementasi Jaringan VPN dengan Routing Protocol terhadap Jaringan Multiprotocol Label Switching (MPLS). Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), 3(1), pp.29-33.
[6] Fathurrahmad, S.Y., Iqbal, T. and Salam, A., 2019. Virtual Private Network (VPN) Network Design For Multiprotocol Label Switching (MPLS) Networks. International Journal of Scientific and Technology Research, 8(11), pp.2653-2656.
[7] Haniza, N., 2019. Pengaruh Media Sosial terhadap Perkembangan Pola Pikir, Kepribadian dan Kesehatan Mental Manusia. J. Komun.
[8] Holik, F., Dolezel, P., Merta, J. and Stursa, D., 2020, September. Development of Artificial Intelligence Based Module to Industrial Network Protection System. In Proceedings of SAI Intelligent Systems Conference (pp. 229-240). Springer, Cham.
[9] Husni, N.L., Handayani, A.S. and Damsi, F., 2017, November. Pelatihan Penggunaan Internet secara Tepat dan Sehat Bagi Guru dan Siswa Di MTS Ar-Rahman Palembang Guna Meningkatkan Kreativitas serta Kesadaran Guru dan Siswa Mengenai Sisi Negatif Internet. In Annual Research Seminar (ARS) (Vol. 3, No. 1, pp. 127-132).
[10] Hwian, C., 2017. Mekanisme Penegakan Hukum Perkara Pidana Pornografi Melalui Internet. Veritas et Justitia, 3(1), pp.117-137.
[11] MikroTik ID. 2020. Blokir Website & File Extention Dengan Web Proxy. URL: http://MikroTik.co.id/artikel_lihat.php?id=123. Diakses tangga 21 Oktober 2020 (11:23).
[12] MikroTik ID. 2020. Implementasi Firewall Filter. URL: http://MikroTik.co.id/artikel_lihat.php?id=57. Diakses tangga 21 Oktober 2020 (10:19).
[13] Muklas, M., Supendar, H. and Sulistianto, S.W., 2020. Optimalisasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Filtering Dan Manajemen Bandwith Pada PT. Intav Prima Solusindo. Tekinfo, 21(1), pp.104-111.
[14] Musyafak, N. and Handayani, M.R., 2018. Implementasi Peraturan Menteri Komunikasi Dan Informatika Nomor 19 Tahun 2014 Dalam Penanganan Situs Internet Bermuatan Negatif (Studi Kasus Pemblokiran terhadap Situs Radikal oleh Kemenkominfo Tahun 2015). Islamic Communication Journal, 2(1), pp.80-99.
[15] Muzakir, A. and Ulfa, M., 2019. Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 10(1), pp.15-20.
[16] Noviansyah, M. and Saiyar, H., 2020. Pemanfaatan Web Proxy Sebagai Pengoptimal Keamanan Jaringan Wireless Lan. Jurnal Khatulistiwa Informatika, 8(1).
[17] Pinariya, J.M. and Lemona, M., 2019. Literasi Internet Ramah Anak. Jurnal Abdi MOESTOPO, 2(02), pp.50-56.
[18] Purwanto, D.D. and Santoso, J., 2015. Multinomial Naïve Bayes Classifier untuk Menentukan Review Positif atau Negatif pelanggan Website Penjualan. In Seminar Nasional "Inovasi dalam Desain dan Teknologi"-IDeaTech 2015
[19] Rahardjo, B., 2005. Keamanan sistem informasi berbasis internet. Jakarta: PT INDOCISC.
[20] Sulaiman, O.K., 2016. Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. Computer Engineering, Science and System Journal, 1(1), pp.9-14.
[21] Suroso, J.T., 2019. Permasalahan Penegakan Hukum Terhadap Situs Internet dengan Konten Negatif Melalui Pemblokiran Situs. Wacana Paramarta: Jurnal Ilmu Hukum, 18(1), pp.39-50.
[22] Suyanto, M., 2005. Pengantar Teknologi Informasi Untuk Bisnis. Penerbit Andi.
[23] Ulinnuha, M., 2013. Melindungi Anak dari Konten Negatif Internet: Studi terhadap Peramban Web Khusus Anak. Sawwa: Jurnal Studi Gender, 8(2), pp.341-360.
[24] Sarno, R., 2009. Audit Sistem Informasi & Teknologi Informasi. Surabaya: ITS Press.