ISSN 2614-0047

Blocking pornography sites on the internet private and university access

Ni'matul Ulfah [a,1,*], Ninon Oktaviani Irawan [a,2], Piska Dwi Nurfadila [a,3], Putri Yuni Ristanti [a,4], Jehad A.H Hammad [b,5]

[a] Department of Electrical Engineering, Universitas Negeri Malang
[b] Computer Information Systems Department, Faculty of Technology and Applied Systems, Al-Quds Open University, Palestine
[1] ulfah153@gmail.com*; [2] ninonirawan@gmail.com; [3] piskadwi12@gmail.com; [4] putriyuni7@gmail.com; [3] jhammad35@hotmail.com
* corresponding author

ARTICLE INFO

Article history
Received January 1, 2019
Revised January 22, 2019
Accepted February 4, 2019

Keywords
Sites
Pornography
Blocking
ISP
Sensor

ABSTRACT

Internet development in Indonesia is not always results in positive effect to the Indonesian people, especially to the learners. By the effect comes from internet application, then, Ministry of Communication and Information Technology conducts blocking activity to the sites suspected to change people's mind. Based on Database of Trust Positive between 2014-2017 type of pornography content has the first place than other contents. The increase of access towards pornography content in Indonesia supported by the availability of reachable internet access. One of contents provides pornography content said that in 2017, the largest user accesses their platform comes from mobile device. It is supported by the price of internet package for mobile device in Indonesia is one of the cheapest than other Southeast Asia countries. Therefore, the government, since 2002 till present, continually conducts blocking activity towards negative sites together with ISP in Indonesia. The ISP (Internet Service Provider) must obey the government by conducting blocking activity towards negative sites through DNS Nawala or other filtering program. The aim of this paper is to analyze pornography access through many types of provider and the differences from each provider in conducting sensor towards sites with pornography content.

1. Introduction

By the reachable internet access that ease people to access internet as well as the increase of internet users from year to year, it is found that one of contents provides pornography content said that in 2017, the largest user accesses their platform comes from mobile device. Data shows that in 2013 the percentage is 45% and becomes 67% in 2017. One of reasons about why the access towards pornography contents popular is the cheap price of internet package for mobile devices. Data from Telecommunications Union shows that rate of data broadband per average GNI per capita in Indonesia is 1.45% cheaper than price in 2015, which is 1.53 per cent. The government realizes that effect caused by pornography can change people's mind, especially learners. Learners still unable to choose content considered as positive or negative content. They will be easier to be affected by their social environment without taking care to the effect of internet using.

According to Law No 44 Year of 2008, pornography is picture, sketch, illustration, photo, text, voice, sound, moving picture, animation, cartoon, conversation, body language, or other messages through many types of communication media and/or performances or shows in the public, which contain sexuality (pornography) or sexual exploitation that violated moral norm prevailed in the society [1]. Pornography is something that arouses sexual desire by picture, painting, photo, video, text or conversation (voice)[2] [3].

In " The Nature And Dynamics Of Internet Pornography Exposure For Youth", it is explained that accessing pornography either through electronic or non-electronic media for them under 18 years old included as a crime [4].

Negative impact caused by pornography to adults is gender believe [5]. In general, pornography has effect to weaken function of each individual and social in the type of mind, body, and heart [6]. Meanwhile, for largest portion of adolescent accesses pornography content is male who already have puberty [7]. In the research, it shows that pornography has negative effect towards learning, which is about content and dynamics of sexual interaction, gender mapped to the sexual relationship, sexual agreement, normalization to the gender violence, and sexual script that create femininity and masculinity.

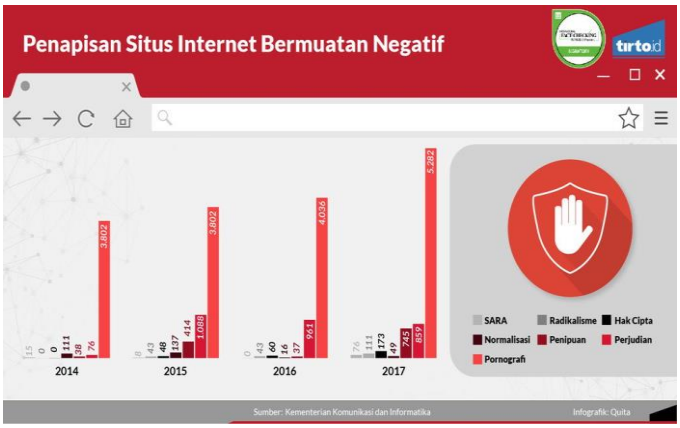

Fig. 1. Negative Internet Site Screening Graphic

Fig. 1 shows the survey in 2014 to 2017 shows that negative contents of pornography group got the first place. The government, in 2002, created program of positive internet in order to cope with negative content of pornography to be followed up with the action.

However, crimes in internet (cyber crime) develop rapidly and still have possibility to access using many ISP in Indonesia in order to access pornography content. Besides that, accessing using proxy and imitating DNS conducted by users to access negative content, especially pornography.

Ministry of Communication and Information Technology realizes the change of people's mind towards internet, thus the Ministry uses reference of Electronic Information and Transaction Laws and Anti-Pornography Laws in order to block sites with pornography contents. Ministry of Communication and Information Technology involves Indonesia Internet Service Provider (APJII) and 15 Internet Service Provider to activate Google Safe Search in Indonesia ISP network. Various internet service providers' result in number and type of content filtered by ISP also various. In order to make standardized control system, Ministry of Communication and Information Technology requires that ISP makes subcontractor of sensor service to assure that each ISP obey the government policy. Ministry of Communication and Information also requires that ISP buys commercial filter product in order to play an active role in controlling contents from ISP administrator.

2. Method

2.1. Interviews

In the process of collecting sites related to pornographic content, interviews were conducted with five speakers. From the five speakers, there are similarities in several sites that are accessed. From the list of sites obtained through interviews both directly and indirectly. The indirect interview method is carried out through WhatsApp. WhatsApp is one of the messaging and exchanging applications commonly used by users in Indonesia. Direct interviews conducted on September 27 only get two sites. Indirect interviews conducted through WhatsApp on September 28th received 21 sites.

2.2. Documentation

The method used to collect material and opinions from the author so that it can be used as a theoretical basis, by analyzing the literature relating to research problems. This method is done for data collection of ISPs who can still access pornographic sites and have been able to access pornographic sites. The collected data is documented in table form. This table is divided into five researches conducted on September 28th, and October 5th, October 12th, October 19th and October 26th. As well as gathering problems on pornographic literature so that it can be presented in the form of methodologies that can underlie this research.

3. Website Filtering

Ministry of Communication and Information Technology runs health and safe internet (INSAN) and TRUST Positive as the attempt to control pornography sites. By those programs, it is expected that it can reduce or erase pornography sites from internet. However, those programs may still considered as centered program due to it is still able to reach controlling in the smallest server unit [8]. Today, the implementation of those programs still optional and many ISP use different techniques in the filtering system. This web filtering can be conducted through three steps, personal, group, and organization. Personal web filtering can be conducted individually through our own computer. Group web filtering is like local network, for example is control application owned by UM. This level of filtering usually conducted through proxy. While, organization web filtering conducted by ISP (Internet Service Provider). ISP included into government method in restricting users to access pornography sites or even blocked it directly through the decision of Ministry of Communication and Information Technology to ISP. The following is many techniques used by ISP to block pornography sites in Indonesia [9].

3.1. DNS Filtering

DNS used in application that connected with internet such as web browser or email. DNS will works by mapping host name to the suitable IP Address [10]. The advantage of this technique is simplicity and effectiveness in case of manipulation. The following stages carried out in the DNS Filtering process describes below [11].

- Rejected, when you want to access a page then a notification appears from the page "Host Not Found" or "Connection Denied".
- NxDomain, manipulate the existence of the host, so when accessing a page "Host Not Found" notification appears.
- Name Hijacking, switch the actual page to a page that is intentionally hijacked to another page.
- Name Invalidation, hijacking web pages by displaying notifications "can't connect".
- Shut up, does not respond to user requests to access the page, resulting in out of time access.
- Provoked server failure, causing a message failure on the user's server to go to a certain domain and displaying the notification "can't connect".

This technique developed to be DNS Nawala in 2009 by the supports from TELKOM in order to implement Laws of Anti-Pornography and Introduction towards “Health and Safe” Program.

3.2. DNS Poisoning and Spoofing

Protection or control program through DNS is a simple level that mostly conducted. As we know about DNS Spoofing [12][13] and DNS Poisoning [13][14] that mostly found such when we access a site but ISP cannot reach the site. This system works like a network cut off, thus it will be seen as if we or the networks are in problem in accessing site. There are many strategies can be conducted through DNS either attack the DNS or protect it using firewall [15].

3.3. Border Gateway Protocol (BGP)

The type of this BGP filtering such as AS_Path Filtering: Peer Locking. Route filtering is basic in regulating BGP policy. There are numbers way to filter one or more network from BGP partner, including information of network layer capability and AS_Path as well as community attribute [16].

There is other feature from BGP that may use, which is Outbond Route Filtering (ORF) feature based BGP Prefix by using BGP ORF to send and receive capability in order to minimize number of BGP update sent between BGP partners. Configuring this feature helps to reduce system resources needed to result and process route update by filtering unwanted route update in the source. For example, this feature can be used to reduce number of processing needed by router that not receive full route from service provider network [17].

3.4. Trust Positive

The attempt conducted to filter contents managed and supported by Ministry of Communication and Information Technology. Principle and technique from this method is saving domain consists of black list and white list as well as configuration information in order to make administrator enable to implement filtering by using open source Squid Cache with Proxy HTTP/caching system with the addition of squidGuard [18].

In the trust site, it has URL delivery page encourages the users to participate in developing URL list used as black list that will be developed by Ministry of Communication and Information Technology.

3.5. Deep Packet Inspection (DPI)

Deep packet inspection is a technology implemented on router that will be used to monitor data in real time. Deep packet inspection is not only observe targeted address, but also payload and sender address. Then, this captured information will be compared with protocol on order to identify data characteristic of ISP hardware. DPI has various functions including [19]:

- Network Security, used by operators to detect malware and also dangerous traffic.
- Network Management, used to handle rare bandwidth. This will make it easier for ISPs to block unwanted traffic such as sharing peer-peer files that consume bandwidth. It can also be used to optimize routing based on the data transferred.
- Surveillance, internet and telecommunications companies in the US use DPI for real-time monitoring needs in collaboration with national security agencies. Besides that it is also used to monitor internet traffic.
- Content regulation, can apply string matching and is used to block websites that are considered dangerous. DPI has the ability to inspect packages.
- Copyright enforcement, can be used to detect copyrighted packages such as music, videos or other copyrighted documents.
- Ad injection, companies like NebuAd and the Phorm package offer ISPs to edit advertisements on websites that are in accordance with the interests of users.

3.6. Application Control dan Url Filtering

Application Control and Url Filtering system was developed by company Check Point. This system has undergone two changes, first in 2014 system was launched as version R76 [20] and the year 2016 named R77 [21]. This application is used to handle Malware and Hogging Bandwidth. The benefits of Application Control and Url Filtering including: (a) Local internet access control to the site that will be on the block, (b) Control bandwidth problem, and (c) Increase security organization. The main feature in the Application Control and Url Filtering are:

- Granular Application Control, identify the website/application is blocked and give protection on malware
- Largest application library with AppWiki, this application uses the library with more than 4500 applications and over 100,000 widgets and Web 2.0 categories that will be on the block.
- Integrated into Security Gateways, enable security gateways i.e. UTM-1, Power-1, IP Appliances, and IAS Appliances.
- Central Management, eases management of security policies
- Smart Event Analysis, helps to understand the proceedings of Application Control and Url Filtering with statistics, reporting filters that pass through security Gateways.

4. Results and Discussion

Strategy to control pornography in Indonesia has been ruled in Laws No 44 Year of 2008, thus government program in blocking sites with pornography contents together with ISP in Indonesia and also content provider itself to remove or block those contents. In this blocking activity, ISP uses site filtering through list given by the government. Despite site filtering, there is DNS blocking for certain sites.

A research conducted by comparing five ISP used in Indonesia and a local application control. This research conducted five times for four weeks; September 28, October 5, October 12, October 19, and October 26 towards 23 sites contained pornography content as with interview to the five persons that ever accessed and still accessing the sites. Such in Table 1, it can be seen the result of research conducted to compare the more secure ISP in sites with pornography content on September 28 to October 26 2018 towards 23 websites.

Table.1 Comparison of 5 ISP Security Against Pornography Sites

P	Observation				
	K1	***K2***	***K3***	***K4***	***K5***
P1	10	10	10	10	10
P2	3	3	3	3	3
P3	9	9	9	9	9
P4	7	7	7	7	7
P5	3	3	3	3	3
University	2	1	1	1	1
Total	34	33	33	33	33

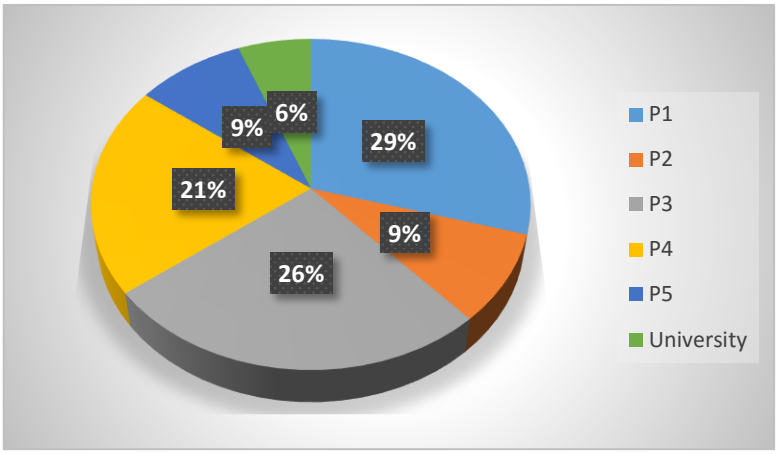

Fig. 2. Diagram of the amount of porn sites from each application.

Based on our research conducted towards five ISP in Indonesia and application as comparison in site blocking, it can be seen in Fig. 2 that from 23 pornography sites ten sites still able to be accessed and 13 sites have been blocked. The following are the results of research on pornographic sites:

- Provider P1 can access ten sites for each study with a presentation of 29% of the total amount of content that can be accessed.
- P2 Provider can access three sites for each study with a presentation of 9% of the total amount of content that can be accessed.
- The P3 Provider can access nine sites for each study with a presentation of 26% of the total amount of content that can be accessed.
- Provider P4 can access seven sites for each study with a presentation of 21% of the total amount of content that can be accessed.
- The University of P5 can access two sites in the first study, while for the four studies, there is a decrease in access, which can access one site with 6% presentation of the total amount of content can be accessed.

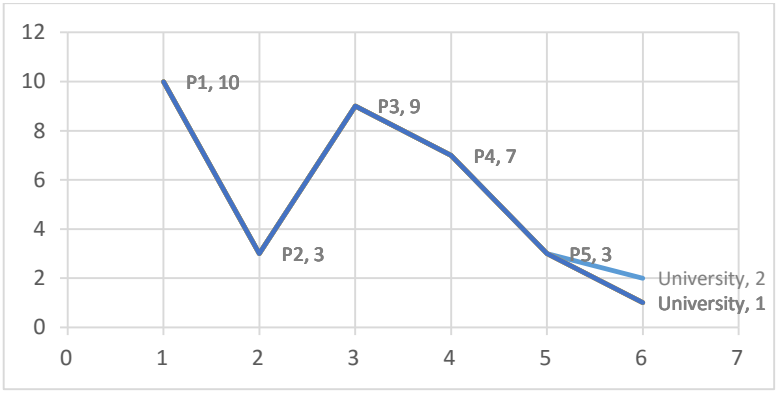

Fig. 3. Graph of changes in the amount of porn sites from each case.

Based on Fig. 3, it can be seen that different color line show research K1-K5 conducted towards porn sites that still able to be accessed as well as provider and application in university. It can be seen each of them, P1-P5, has no change towards its number of porn sites can be accessed, where it is shown from color of K1-K5 research that overlapped each other. Meanwhile, in accessing sites through university, it shows a change. There is change from two sites that still able to be accessed become only one site that still able to be accessed. Then, in Fig. 4, it shows change towards number of porn sites that still able to be accessed from the whole research.

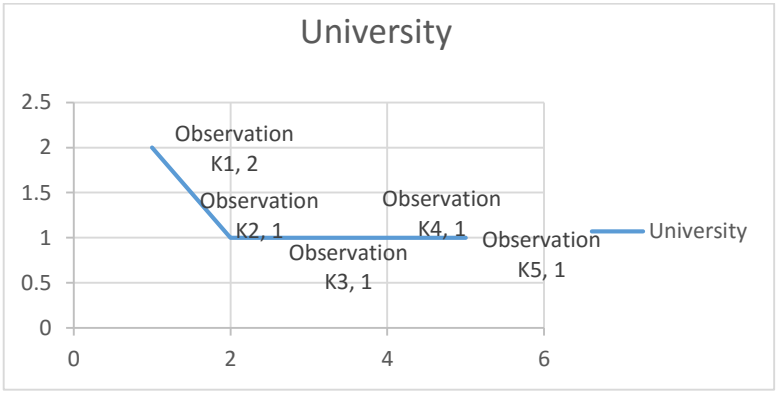

Fig. 4. Graphic of changes in the amount of porn sites from the university network.

The difference of pornography sites that able or unable to be accessed by provider caused by the difference of technique and filtering system used by Internet Service Provider. Table 2 presents filtering technique owned by provider or university used to block pornography sites.

Table.2 Comparison of 5 ISP Methods to Pornography Sites

P	Methods				
	A	***B***	***C***	***D***	***E***
P1	√	-	√	-	-
P2	-	-	√	-	-
P3	-	-	√	-	-
P4	-	-	-	-	-
P5	-	√	√	√	-
University	-	-	-	-	√

[a] A: DNS Filtering
[b] B: DNS Poisoning and Spoofing
[c] C: BGP (Border Gateway Protocol)
[d] D: Trust Positive
[e] E: Application Control and Url Filtering

The research result shows that provider P5 gets highest portion to use blocking method of DNS Poisoning and Spoofing, BGP (Border Gateway Protocol) and Trust Positive. Method development conducted by provider P5 able to block 20 pornography sites. The research result also shows that

provider P4 uses those three blocking the techniques as well as this is directly proportional to the amount of content that is successfully blocked.

For example provider P1 uses proxy or gateway blocking technique, then the mechanism of blacklist internet access will give notification in the cellphone screen with notification of "access is denied to security policy enforcement'. While, provider P5 uses blocking technique of Trust Positive by mechanism of creating specific team to look for safe sites to be accessed or included into whitelist and unsafe sites to be accessed or included into blacklist. Besides that, those provider companies also open to the input from customers relate to sites that must be blocked to be directly included into blacklist.

The Research result that the University uses a third party to block pornographic sites namely Application and url filtering, with the workings of the University party input the url of the content that is considered as containing pornography.

5. Conclusion

From the research that we have done, there are 23 pornographic sites out of five interviewees that we have interviewed. Of the 23 sites tested using five different ISPs. The results obtained are not all providers can access the site, there are differences between one provider and another provider, and this is because each provider has its own technique in blocking pornographic sites. This study also examines the techniques carried out by providers in blocking, from the analysis that we got, there are four techniques used by providers namely DNS Filtering, DNS Poisoning and spoofing, BGP, Positive Trust, and Application Control & URL filtering. The difference between the four sites is the costs that will be incurred from ISPs in blocking pornographic sites.

References

[1] Kementrian Hukum dan HAM, "UNDANG-UNDANG RI NOMOR 44 TAHUN 2008 TENTANG PORNOGRAFI." 2008.

[2] E. W. Owens, R. J. Behun, J. C. Manning, and R. C. Reid, "The Impact of Internet Pornography on Adolescents : A Review of the Research," *Sex. Addict. Compulsivity*, vol. 19, pp. 99–122, 2012.

[3] J. K. Global, P. Prihandini, P. A. Janitra, and U. Padjadjaran, "Perilaku penggunaan smartphone dan akses pornografi di kalangan remaja perempuan," *J. Komun. Glob.*, vol. 7, no. 1, pp. 1–11, 2018.

[4] C. Sabina, J. Wolak, and D. Finkelhor, *The Nature and Dynamics of Internet Pornography Exposure for Youth*, vol. 11. 2008.

[5] P. J. Wright, R. S. Tokunaga, and A. Kraus, "A Meta-Analysis of Pornography Consumption and Actual Acts of Sexual Aggression in General Population Studies A Meta-Analysis of Pornography Consumption and Actual Acts of Sexual," *J. Commun.*, no. 66, pp. 183–205, 2016.

[6] T. Rahmania and H. C. Haryanto, "Persepsi pornografi pada anak (studi pendahuluan pada siswa kelas 5 sekolah dasar islam 'x')," *Inq. J. Ilm. Psikol.*, vol. 8, no. 1, pp. 55–74, 2017.

[7] G. Dines, "Dignity: A Journal on Sexual Exploitation and Violence Growing Up With Porn: The Developmental and Societal Impact of Pornography on Children," *Dign. A J. Sex. Exploit. Violence*, vol. 2, no. 3, pp. 1–9, 2017.

[8] M. A. Helmiawan and S. Kom, "Internet Sehat Dengan Metode Web Filtering Layer 7 Pada Jaringan Wireless(Study Case Hotspot RT4 Cipeuteuy Baru)," no. April, 2018.

[9] R. A. Halimatussa, Y. Hasan, and L. Belakang, "Analisa akurasi," vol. 4, no. September, pp. 68–74, 2012.

[10] R. D. Sari, A. P. U. Siahaan, Supiyandi, and M. Muttaqin, "A Review of IP and MAC Address Filtering in Wireless Network Security," *IJSRST (International J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 470–473, 2017.

[11] R. Scott and A. Melgosa, "Using Blocking / Filtering Technologies," *J. Advent. Educ.*, vol. 1, no. March, pp. 55–67, 2013.

[12] N. Tripathi, M. Swarnkar, and N. Hubballi, "DNS Spoofing in Local Networks Made Easy," in *IEEE International Conference on Advanced Networks and Telecommunications Systems*, 2017.

[13] A. Polyakov, "DNS Spoofing and Poisoning : Trust , Danger , and Solutions." .

[14] H. S. Hmood, Z. Li, and H. K. Abdulwahid, "Adaptive Caching Approach to Prevent DNS Cache Poisoning Attack," *Comput. J.*, vol. 58, no. 4, pp. 973–985, 2015.

[15] J. Afonso and P. Veiga, "Improving DNS Security Using Active Firewalling with Network Probes," *Int. J. Distrib. Sens. Networks*, vol. 8, no. 5, p. 684180, May 2012.

[16] CISCO, "Identifying and Filtering Routes based on NLRI Filtering Using distribute-list with a Standard Access List," .

[17] CISCO, "BGP Prefix-Based Outbound Route Filtering," in *IP Routing: BGP Configuration Guide, Cisco IOS Release 15M&T*, 2017.

[18] C. Andersen, "Tinjauan Hukum Kewenangan Sistem TRUST + POSITIF ™ sebagai Database Acuan dan Rujukan Penyaringan Seluruh Layanan Akses Informasi Publik Penggunaan Internet di Indonesia," *Dialogia Luriduca J. Huk. Bisnis dan Investasi*, vol. 9, no. 1, pp. 80–91, 2017.

[19] R. Bendrath, "Global technology trends and national regulation : Explaining Variation in the Governance of Deep Packet Inspection," *Int. Stud. Annu. Conv.*, no. February, pp. 1–32, 2009.

[20] Check Point, *Application Control and URL Filtering R76*, no. April. 2014.

[21] Check Point, *Application Control and URL Filtering R77*, no. December. 2016.