Strategy To Block Traffic Create By Anti-Censorship Software In LAN for Small and Medium Organisation

Kamal Harmoni Kamal Ariff, Baharudin Osman
UUM, Malaysia
kamal@kamalharmoni.com, bahaosman@uum.edu.my

Abstract- Anti-censorship software originally develop to fight internet censorship in China. The anti-censorship software such as Ultrasurf, Freegate, Gpass, GTunnel and FirePhoenixare become popular for the stubborn user who used the internet for thier own's purpose and disobey the poilicies . Since it is widely use by users in organisation local area network to bypass firewall policies, it become a threat to LAN organization. Hence, it cause a problem for network administrator who manage the internet utilisation and enforcing internet policies. For an organisation, uncontrolled internet usage lead the opened system vulnerability to viruses, backdoor, non-productivity activities and slow internet connection. Thus, this studies proposed strategies to filter and blocking traffic create by anti-censorship software in LAN. Method used in this project is ***"design computer security experiment"****. Therefore, this project will guide the network administrator to control internet utilisation, protect organisation LAN and carried out implementation of the internal organization's internet policies.*

I. INTRODUCTION

Computer technologies are changing rapidly. In the organization of LAN, to prevent users from accessing restricted web site and conduct activities such as downloading movie and accessing pornography web site has become a common internet policy. A war between network users and network administrator is never ending. Users will find a way or strategies to bypass firewall and network administrator will find a way to block and implement internet policy to protect LAN. Referring to (Aycock & Maurushat, 2008), "by using anti-censorship client software user are able to bypass firewall in LAN". There many choices of anti-censorship software in the market. According the Global Internet Freedom Consortium (GIFC, 2010), some example of Anti-censorship software are Ultrasurf, Freegate, Gpass, GTunnel and FirePhoenix. Internet censorship is a common practice among organization now days. According to Wikipedia (2010), censorship has define as "the use of state or group power to control freedom of expression, such as passing laws to prevent media from being published, propagated and access." However, for this studies censorship is define as "The use of group power to control freedom of accessing web services". In organization, task to implement internet censorship is given to network administrator.

Network administrator need to monitor and control internet activities for the benefit of organization. In organization if users used anti-censorship software they can bypass an organization firewall. Network administrator should block users that had been used anti-censorship software from bypass firewall and access internet restricted website. Ensuring the users were not be able to access restricted web site via anti-censorship software, required a system. The system functionally able to do traffic analysis and need to be execute at firewall level. Thus, the firewall is functionally to reject traffic requests from client that was using anti-censorship software while surfed. According to Becchi & Crowley, (2007), "firewalls with Deep Packet Inspection

(DPI) capabilities are able to block traffic request from anti-censorship software". Somehow to have firewall with this DPI capability was expensive for a small organization. The purpose of conducting this study will carried out a strategy to filter and blocking traffic request from anti-censorship software which are able to used by a small organization at affordable cost.

II. Problem Statement

Ultrasurf became the most common anti-censorship application that has been used in LAN to bypass firewall. Ultrasurf communicated to target server using external proxy's server. IP addresses of all external proxies were always changes. It was very hard to do traffic filtering and blocking base on each proxies IP address. This required another strategy that able to do filtering and blocking. Ultrasurf used port 443 (https) and 80 (https) to communicate from user computer to external proxies server through an organization firewall. Since not many firewalls able to filter traffic request that went through https protocol, filtering this traffic was difficult to be done. Therefore, only the commercial firewall which is expensive able to provided filtering and blocking https packet. These required a solution that suitable for small organization to implement, which is less expensive and affordable. Thereby created a strategy on how to filter and block Ultrasurf traffic, transform the network administrator ability to control internet utilization and carried out implementation of internet policies. Network administrator also needs to ensure network is used for the benefit to all users in the organization.

III. Literature review

Anti-censorship software such as Ultrasurf, freegate, gpass, garden, GTunnel, and FirePhoenix are software that can bypass firewall. Arccording to Wikipedia (2010), the most commonly website block by firewall are Pornographic, Social networks (e.g. Facebook, MySpace and Twitter) , Political blogs, YouTube, Nazi and similar websites and Religious websites. User will used anti-censorship software to be able to access listed category of web page. There is many anti-censorship software in the internet and some of them is fee to use. Arcoding to Global Internet Freedom Consortium, Ultrasurf are the most commonly use (GIFC, 2010) and Arccording to Kaiser, (2008) Ultrasurf was state as "Possible as The Best Proxy Server, 2008".

IV. Research Objectives

The aim of this study is to blocking traffic created by Ultrasurf from LAN to internet. In order to achieve the main objective, the specific objective has been planned as follows:

1. To identify how Ultrasurf connect to internet.
2. To produce strategy to block traffic created by Ultrasurf
3. To evaluate the strategy.

V. Why Ultrasurf hard to detect and block

Recently, Ultrasurf not only been used in China to bypass the "golden shield project", but it also been used in LAN that applied internet restriction. By using Ultrasurf, users inside organization LAN are able to bypass firewall and access restricted website. According to Xia (2004), "Ultrasurf is extremely difficult to block". Ultrasurf is using port 9666 to communicate from web browser to the Ultrasurf services, but communication using this port only at local computer. Blocking this port at organization firewall will not function. Ultrasurf uses a secure socket layer (SSL) to communicate from local computer to their proxies. They have thousands of proxies, which mean to block IP proxies are not practical. It is not suitable because from time to time many more IP address being increasing in the list. It also used Port 443 and cannot be block at firewall. This is because Port 443 use for https communication. However, if this port is been blocked, website such mail.yahoo.com, Gmail.com and banking online system that used this secure socket layer to communicate failed to work.

VI. any firewall able to block Ultrasurf?

As mention in introduction, there are firewalls that able to block Ultrasurf. According to Kumar, Turner, & Williams (2006) and Piyachon & Luo (2006), filteration can be done

by using SSL interceptor and perform DPI (deep packet inspection). Firewall that have DPI capabilities are able to filter traffic that come from anti-censorship software. This means it also able to block Ultrasurf. There are commercial firewalls that able to block anti-censorship software, but they are expensive. Example of firewall that has this kind of capability is Sonic Wall and Symantec firewall. This type of firewall was considered expensive firewall for small and medium organization. For this project, open source solution is preferable since it is free for everyone.

VII. METHODOLOGY

The analysis of this study will be divided into 7 main phases. This methodology is adapted from (Peisert & Bishop, 2007). This methodology has be use for "How To Design Computer Security Experiment". For this studies the "Propose strategy" and "Validate hypothesis" phase was added. This change is made suite studies that will be conducted. Below are methodology used by peisert and bishop.

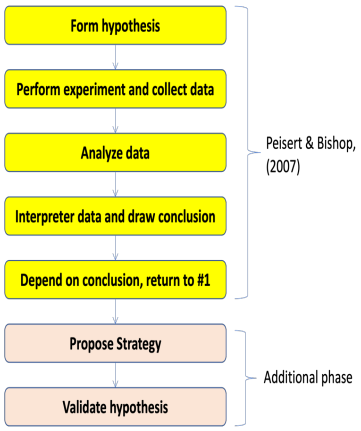

Figure 1 : Methodology used in this studies

Phase 1 : Form Hypothesis

This phase will form the hypothesis. To form hypothesis information will be getting from literature review. To identify requirement for blocking Ultrasurf connection, the process of web accessing from Ultrasurf is listed.

Table 1 : Process of connection and location it happen

Process of connection	Location	Ability to control by network admin
Web browser connect to Ultrasurf using localhost (ip 127.0.0.1) port 9666 and create as local proxy server.	Local Computer	No
Ultrasurf (discovery agent) connect to various external IP (external proxies server) using port https (443) and http (80).	LAN to WAN via Gateway	Yes
External proxies server will connect to restricted web site and passing back to proxies server.	WAN	No
Proxies server will encrypt (if using port 443) the content and send back to Ultrasurf (discovery agent).	WAN to LAN Via Gateway	Yes
Ultrasurf as local proxy server will pass the content to web browser.	Local Computer	No

The requirement to block ultra surf is identified. Process of "Ultrasurf (discovery agent) connect to various external IP (external proxies server) using port https (443) and http (80)." This process will use organisation gateway to go to internet. This process happen inside organisation and under supervise by network admin. In normal organisation gateway used to connect to internet. It become a centre for every computer in LAN use this gateway to connect to internet. These processes are identified as place to studies and conduct experiment, since it locate in the area where is controllable and centralize. As an outcome form this phase, a hypothesis "*it is possible to block Ultrasurf if how it connect to internet is identify*".

Phase 2 : Perform Experimentation And Collect Data.

This phase carried out the possibilities by creating simulation to test. All the findings will be recorded. This phase is to gather information how Ultrasurf connect to internet. Experiment being conduct in 4 conditions :

a) Firewall **at router** block specify domain name **without** Ultrasurf installed and label as Exp : 1.
b) Firewall **at Squid proxies** block specify domain name **without** Ultrasurf installed and label as Exp : 2.
c) Firewall **at router** block specify domain name **with** Ultrasurf installed and label as Exp : 3.
d) Firewall **at Squid proxies** block specify domain name **with** Ultrasurf installed and label as Exp : 4.

All four (4) experiments were using 100 domain names for data sampling. Fifty (50) black list domains name was label as "Black list domain" and remaining fifty (50) labels as "white list domain". Blacklist domain was enter into firewall to block connection request from client.

Phase 3: Analyze Data.

Result of each experiment result was captured and labelled as below.

Table 2 : Result Of Experiment

Domain Name	Exp: 1	Exp: 2	Exp: 3	Exp: 4
White List Domain	Yes	Yes	Yes	Yes
Black List Domain	No	No	Yes	Yes

Tables 2, Experiment 3 and 4 show that client installed with ultrasurf able to bypass router firewall and proxies firewall. Form figure 3, Packet analyser show that ultrasurf using port 80 and 445 and connect to various IP of external proxies server.

Phase 4: Interpreter and Draw conclusion

In this phase, it was confirm that it's possible to block traffic create by Ultrasurf as shown in previous phase, that it use http and https port to communicate with outside server and Ultrasurf used various IP that become Ultrasurf external proxies. This phase suggest that by blocking communication trough IP. It will block Ultrasurf connection. On this phase **objective 1 "To identify how Ultrasurf connect to internet" has been achieve**

Phase 5: Conclusion Based On The Experiment.

Based on the outcome from interpret phase, the data drawn as conclusion. It support and agree with the hypothesis of this studies. Analysis from captured packet has showed:

1. Ultrasurf connected to various external IP address.
2. Connect used port 80 (http) and port 443 (https).
3. It uses TCP protocol for communication.

Phase5: Propose Strategy

Based on all sources from the conclusion of the experimentation, this phase exposed a strategy on how to filter and block Ultrasurf. The guidelines are listed. All captured packet generated by Wireshark has been analysed. As an outcome from previous phase, one strategy has been established is:

"To reject ALL traffic using TCP protocol port 80 and 445 that try to connect based on IP address."

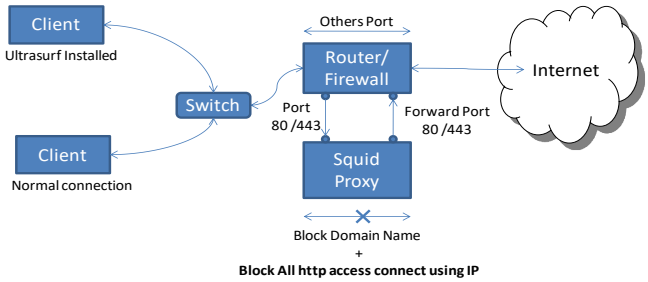

Figure 2: Propose System

Tables 3, Show that ultrasurf using port 80 and 445Experiment 3 and 4 show that client installed with ultrasurf able to bypass router firewall and proxies firewall. In Squid proxy server can has configured as follow

```
acl blacklist_domain_contain url_regex -i
"/etc/squid/blacklist_domains_contain.acl"

acl blacklist_domain dstdomain
"/etc/squid/blacklist_domain.acl"

acl access_by_ip url_regex \b(25[0-5]|2[0-4][0-
9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-
9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-
9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b

http_access deny access_by_ip
http_access deny blacklist_domain
http_access deny blacklist_domain_contain
http_access allow all
```

Figure 3: squid.conf

From the Figure 3 above, the importance squid parameter is "acl access_by_ip url_regex \b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b". Parameter "http_access deny access_by_ip" was used to filter all http and https access. This mean squid will deny user that try to connect to access http and https using IP address as URL.

```
.bigfishgames.com
.roadandtrack.com
.sex.com
.youtube.com
```

Figure 4: squid.conf

```
Games
horny
porn
games
sex
```

Figure 5: blacklist_domains_contain.acl

Figure 4 and Figure 5 show additional file to support squid to blocked specific domain and any domain contained specific word in their domain name. **On this phase objective 2 "To produce strategy that able to block Ultrasurf" has been achieve.**

Phase 6: Validate The Hypothesis

Strategies that been applied into an organisation firewall and the effect been analysed and conclude either the strategies is working or not. Based on the proposed strategy that been used, Experiment 4 (Web filtering at squid with Ultrasurf Installed) has been conducted again to validate the requirement needed.

Table 3 : Validate Result

Domain Name	Exp: 1	Exp: 2	Exp: 3	Exp: 4
White List Domain	Yes	Yes	-	Yes
Black List Domain	No	No	-	No

Table 3 showed result from experiment after propose strategy to block Ultrasurf has applied.

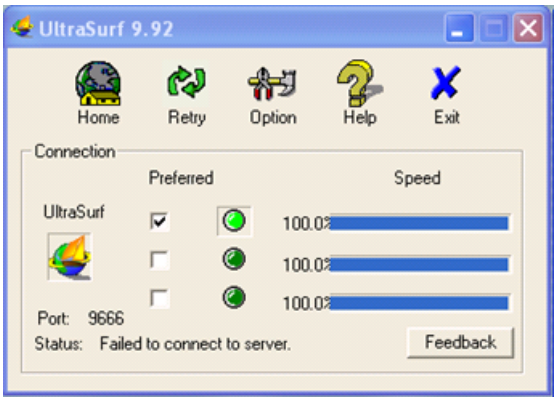

Figure 6: Ultrasurf unable to connect to internet

Figure 6 has showed that Ultrasurf unable to connect to external IP. All white list and black list domain cannot be accessed by user even those Ultrasurf was installed in their PC. This showed that user installed with Ultrasurf unable to

access internet. Since this strategie cannot be applied inside firewall, Experiment 3 cannot be conduct.

VIII. CONCLUSIONS

After the experiment conducted, most of the firewall is unable to block anti-censorship software such as Ultrasurf. A strategy to combat anti-censorship should be introduced to protect organization. This project has been introduced a strategy to block user from accessing prohibited website. Squid proxy server has ability to provide a blocking IP address based on http and https connection. From these studies two techniques of implementation is proposed.

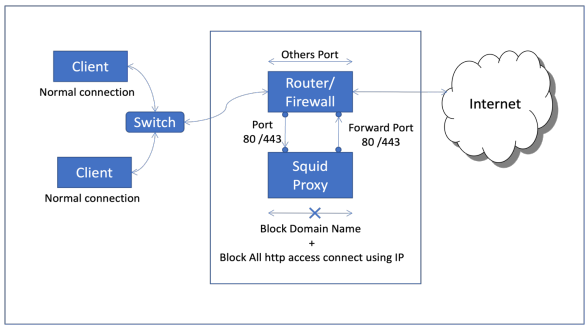

Figure 7: Router, Firewall and Proxy In a Box

From the figure 7, it show the strategy to implementing restricting accessing website in single box. This box act as router / firewall and proxies.

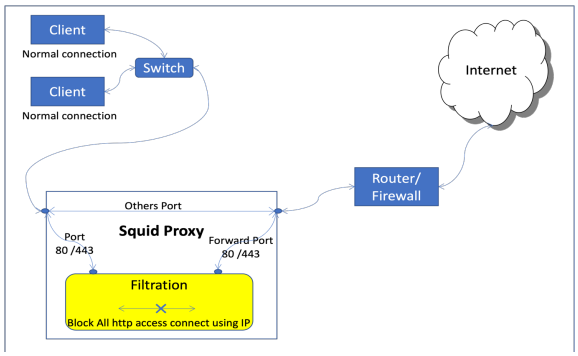

Figure 8: Independent Proxy

Figure 8 was proposed since this strategy was used squid to filter and block. Base on Experiment 3 (*Firewall* ***at router*** *block specify domain name* ***with*** *Ultrasurf installed).* This strategy cannot be applied directly in router or firewall. As show on figure 8 Strategy was applied outside a router/ firewall to filter and blocking ultrasurf. The key for this strategy is "***To reject ALL traffic using TCP protocol port 80 and 445 that try to connect based on IP address.***" " these mean if user try to connect to internet using http or https it must use domain name, If user using IP address Squid will drop this network traffic request. Squid also able to be configure to allow connection using specific IP address. Squid as proxies server play a vital role on this strategy

IX. FUTURE DEVELOPMENTS

This strategy of blocking Ultrasurf traffic request can be enhanced in many ways and there will always be new developments evolve in this anti-censorship technology. These reveal the new areas for researchers to explore. The following entries will briefly present the further enhancements specification:

i. **Performance.**

This research studies never touch about performance to process of the filtering traffic request. For an example, what will happen if 1000 user request at same time. Is squid server able to support and what is the best hardware specification to handle connection efficiently?

ii. **Squid new technology.**

Squid proxy server keeps updating their feature to meet the user's target. A question of "Are current squid configuration (Squid.conf) are working perfectly in all version of squid need to be answer.

iii. **Network model.**

In this project, traffic filtration is a key to block Ultrasurf traffic. Due to time constrain, only squid has be study to provide the traffic filtering. IPTables also can provide traffic filtering. How to use same concept and applied at IPTables phase.

iv. **Others type of anti-censorship software**

As mentioned in chapter 1, there are five (5) anti-censorship software available in the marker. The software are Ultrasurf, Freegate, Gpass, GTunnel and FirePhoenix. In these studies only Ultrasurf has been tested. By using the same strategy it may work on others anti-censorship software as well.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Ali Yusny, Nuraini Ahmad, Rahman Zakaria, Raduan Said and finally Anisah Ahmad for their involvement and support during the development of the studies.

REFERENCES

About Us - Global Internet Freedom Consortium. (2010). Retrieved 01 05, 2010, from http://www.internetfreedom.org/about

Aycock, J., & Maurushat, A. (2008, March). "Good" worms and human rights. *SIGCAS Computers and Society, Volume 38 Issue 1* .

Becchi, M., & Crowley, P. (December 2007). A hybrid finite automaton for practical deep packet inspection. *CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference.* ACM.

GIFC. (2010). Retrieved 01 05, 2010, from About Global Internet Freedom Consortium: http://www.internetfreedom.org/

Hunter, C. D. (April 2000). Internet filter effectiveness (student paper panel): testing over and underinclusive blocking decisions of four popular filters. *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions.* ACM.

Kaiser, A. (2008, Aug 12). *technopedia*. Retrieved 01 05, 2010, from UltraSurf : Probably The Best Proxy Server Ever!!!: http://technopedia.info/tech/2008/08/12/ultrasurf-probably-the-best-proxy-server.html

Kumar, S., Turner, J., & Williams, J. (December 2006). Advanced algorithms for fast and scalable deep packet inspection. *ANCS '06: Proceedings of the 2006 ACM/IEEE symposium on Architecture for networking and communications systems.* ACM.

Peisert, S., & Bishop, M. (2007). how to Design Computer Security Experiments. *Springer Boston. Volume 237/2007*, pp. 141-148. Springer Boston.

Piyachon, P., & Luo, Y. (December 2006). Efficient memory utilization on network processors for deep packet inspection. *ANCS '06: Proceedings of the 2006 ACM/IEEE symposium on Architecture for networking and communications systems.* ACM.

Regular Expressions.info. (2010). Retrieved 4 20, 2010, from Sample Regular Expressions: http://www.regular-expressions.info/examples.html

Reuters. (2007, July 18). Retrieved 01 05, 2010, from Chinese Internet censors blamed for email chaos: http://www.reuters.com/article/idUSPEK9185520070718

Strange Maps. (2007, 8 3). Retrieved 3 20, 2010, from A Map of the Internet's Black Holes: http://strangemaps.wordpress.com/2007/08/31/170-a-map-of-the-internets-black-holes/

Tan, Z. A., Mueller, M., & Foster, W. (1997). China's new Internet regulations: two steps forward, one step back. *Communications of the ACM archive* , 11 - 16.

Whitten, J. L., Bentley, L. D., & Dittman, K. (2004). *System Analysis and Design Method. 6th ed.* Boston: Mc-Graw-Hill Education.

Wikipedia. (2010a). Retrieved 01 05, 2010, from Internet censorship: http://en.wikipedia.org/wiki/Internet_censorship

Watt, A. (2005). *Beginning Regular Expressions.* John Wiley & Sons

Xia, B. (2004). The Coming Crash Of The Matrix. *China Right Forum* , pp. 42-44.