ACCESS CONTROL LIST CONFIGURATION TO BLOCK ANTI-CENSORSHIP SOFTWARE IN HIGHER EDUCATION INSTITUTIONS IN MALAYSIA

School of Computing
UUM College of Arts and Sciences
Universiti Utara Malaysia

bahaosman@uum.edu.my[1]
azizia@uum.edu.my[2]
osman@uum.edu.my[3]

Kamal Harmoni

Kedah Industrial Skills and Management Development Centre
Malaysia

kamalharmoni@yahoo.com

ABSTRACT

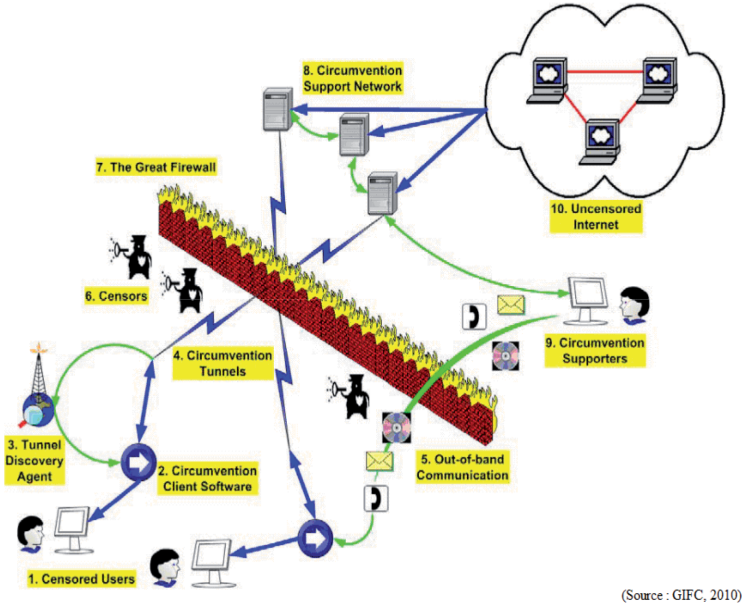
Anti-censorship software was originally developed to fight internet censorship in China. A anti-censorship software such as UltraSurf, Freegate, Gpass, GTunnel and FirePhoenix became popular with stubborn users who used the Internet for thier own purposes and disobeyed the organization's policies. Statistics show that Facebook, and YouTube are ranked as the most popular websites used by college students in Malaysia. Since they are widely used by users in the local area network to bypass firewall policies, they have become a threat to the LAN organization. Hence, it causes a problem for network administrators who manage internet utilisation and enforce internet policies. For an organisation, uncontrolled internet usage leads the open system to be vulnerably to viruses, backdoor, non-productivity activities and slow internet connections. Thus, this study proposes a strategy to filter and block traffic created by anti-censorship software in LAN. The method used in this project is the "design computer security experiment". Therefore, this project will guide the network administrator to control internet utilisation, protect the organisation's LAN and carry out the implementation of the internal organization’s internet policies. As a result, this paper has proposed a strategy to block the UltraSurf anti-censorship software.The proposed strategy was tested in several public and private higher education institutions.

Keywords: Anti-censorship, block traffic, UltraSurf.

INTRODUCTION

Nowadays, computer technologies are changing rapidly. In the organization of LAN, to prevent users from accessing restricted websites and conducting activities such as downloading movies and software, and accessing pornography, Facebook and Twitter websites have a common internet policy. Peer-to-Peer (P2P) applications such as BitTorrent can steal bandwidth and bring with them all kinds of mischievous files. Accessing streaming video sites such as Youtube.com consumes a lot of bandwidth. University students either in public or private education institutions will try to access these entirely restricted websites although they have been blocked by the firewall. Heavy traffic will slow down the network performance if this restricted website is open especially for downloading a movie, facebook or twitter. According to Danyaro et al. (2010), Facebook, YouTube and Wikipedia are ranked as the most popular websites used by college students. From their study, statistically, they estimated that between 32.90% and 43.06% of college students use Facebook on a daily basis, compared to YouTube’s 13-22% and Wikipedia’s 6.87–13.13%. A war between network users and network administrators is never-ending. Network administrators will find a way to block and implement internet policies to protect the router, firewall or proxy to prevent users from accessing these restricted websites. However, users will find ways or strategies to bypass the firewall. According to Aycock & Maurushat (2008), by using anti-censorship client software users are able to bypass firewall in LAN. There many choices of anti-censorship software in the market. According to the Global Internet Freedom Consortium (GIFC, 2010), some examples of anti-censorship software are UltraSurf, Freegate, Gpass, GTunnel and FirePhoenix. Internet censorship is a common practice among organizations nowadays.

According to Wikipedia (2010), censorship is defined 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 accessed”. However, for this study censorship is defined as “the use of group power to control freedom of accessing web services”. In an organization, the task to implement internet censorship is given to the network administrator. The network administrator needs to monitor and control internet activities for the benefit of the organization. In an organization if users used anti-censorship software they can bypass an organization is firewall. The network administrator should block users who anti-censorship software to bypass firewall, and restricted access to the website. As a solution, a system is required to ensure the users are not able to access restricted websites via anti-censorship software. The system should be able to do traffic analysis and need to be executed at the firewall level. Normally, the firewall is used to reject traffic requests from clients that use anti-censorship software while surfing. According to Becchi and Crowley (2007), firewalls with Deep Packet Inspection (DPI) capabilities are able to block traffic requests from anti-censorship software. Somehow to have firewall with this DPI capability is expensive for a small organization


8. Circumvention Support Network
7. The Great Firewall
10. Uncensored Internet
6. Censors
9. Circumvention Supporters
4. Circumvention Tunnels
3. Tunnel Discovery Agent
2. Circumvention Client Software
5. Out-of-band Communication
1. Censored Users

(Source : GIFC, 2010)

Figure 1. Anatomy of anti-censorship system.

According to GIFC – white paper, "The ultimate function of an anti-censorship system is to connect censored users to the uncensored internet server securely and anonymously". Figure 1 shows how anti-censorship works. That shows the general concept of the anti-censorship system step by step. Censored users (1) are normal users in LAN or in a country. User-used circumvention-client software (anti-censorship software) is installed in a censored user's computer. This client software has the ability to connect to the out side and also connect to the circumvention tunnels (4). Basically, it uses the tunnel discovery agent (3) to connect the software to the circumvention tunnel. Once it is connected, the network traffic automatically is encrypted before being connected to the outside by penetrating the GFW (7). Usually the censors (6) are not able to detect this kind of traffic because it is encrypted. Once outside the GFW (7), the network traffic then enters into a circumvention-support network (8). This circumvention-support network is set up and operated by anti-censorship supporters (9) who have many supporters and setups via many infrastructures. The computer in this circumvention-support network (8) acts as proxies. Proxies access the content from unstructured internets (10) and the target server. The target server then sends the information back to the route. The information traffic does not necessarily take the same route that it took to it come. It can be a different route to reach the censored user's computer. Initially if a censored user knows nothing about the other side of the GFW, it is necessary to get them bootstrapped by employing out-of-band communication channels (5). The channels include emails, telephone calls and instant messages. Sometimes users can also take advantage of these channels to locate circumvention tunnels (4), if the client software used does not have a tunnel discovery agent (3). In fact the most important component in the anti-censorship system is the tunnel discovery agent (3). With such an agent, a user does not need to configure the software. The agent automatically finds circumvention tunnels for the user. This study carried out a strategy to filter and block traffic requests from anti-censorship software which can be used by small organizations at an affordable cost.

PROBLEM STATEMENT

UltraSurf became the most common anti-censorship application used in LAN to bypass firewall. UltraSurf communicates with the target server using the external proxy's server. IP addresses of all external proxies always change. It is very hard to do traffic filtering and block the base on each proxy IP address. This requires another strategy that is able to do filtering and blocking. UltraSurf uses port 443 (https) and 80 (http) to communicate from user computer to the external proxies server through an organization is firewall. Since not many firewalls are able to filter traffic requests that go through the https protocol, filtering this traffic is difficult. Therefore, only the commercial firewall which is expensive is able to provide filtering and blocking https packets. These require a solution that is suitable for small organizations to implement, which is less expensive and affordable. To create a strategy on how to filter and block UltraSurf traffic, transform the network administrator's ability to control internet utilization and carry out the implementation of the internet policies. The network administrator also needs to ensure the network is used for the benefit of all users in the organization.

LITERATURE REVIEW

Anti-censorship software such as UltraSurf, Freegate, Gpass, Garden, GTunnel, and FirePhoenix are software that can bypass firewall. According to Wikipedia (2010), the most common website blocks by firewall are pornographic, social networks (e.g. Facebook, MySpace and Twitter), political blogs, YouTube, Nazi and similar websites and religious websites. User used anti-censorship software are used to access some listed categories of websites. There are many anti-censorship software in the internet and some of them are free to use. According to Global Internet Freedom Consortium, UltraSurf is most commonly used (GIFC, 2010) and according to Kaiser (2008) UltraSurf is stated as "Possible as The Best Proxy Server, 2008".

Recently, UltraSurf has not only been used in China to bypass the "golden shield project", but it also has been used in LAN that applies internet restriction. By using UltraSurf, users inside the organization's LAN are able to bypass the firewall and access the restricted website. According to Xia (2004), "UltraSurf is extremely difficult to block". UltraSurf uses port 9666 to communicate from the web browser to the UltraSurf services, but communication using this port is only in local computers. When this port is blocked at the organization, firewall will not function. UltraSurf uses a secure socket layer (SSL) to communicate from the local computer to their proxies. They have thousands of proxies, which means blocking IP proxies is not practical. It is impossible because from time to time many more IP addresses are being added to the list. It also uses port 443 and cannot be blocked at the firewall because this port is used for https communication. However, if this port is blocked, websites such yahoo.com, gmail.com and banking online systems that use this secure socket layer to communicate fail to work.

As mentioned in the introduction, there are firewalls that are able to block UltraSurf. According to Kumar, Turner, & Williams (2006) and Piyachon & Luo (2006), filteration can be done by using the SSL interceptor and performing DPI (deep packet inspection). Firewalls that have DPI capabilities are able to filter traffic that comes from anti-censorship software. This means it is also able to block UltraSurf. There are commercial firewalls that are able to block anti-censorship software, but they are expensive. Examples of firewalls that have this kind of capability are Sonic Wall and Symantec firewall. These types of firewall are considered expensive for small and medium organizations. For this project, the open source solution is preferable since it is free.

According to UltraReach Internet Corp, UltraSurf is one of the most successful anti-censorship software in the world. It is a green software, no installation process is needed and no change in the system setting is required.

UltraSurf enables users in countries with heavy Internet censorship to visit any public website in the world safely and freely- just the same as using the regular IE browser– while it automatically searches the fastest proxy servers in the background. It has strong support for load balancing and fault tolerance, and it even employs a decoying mechanism to thwart any tracing effort of its communication with its infrastructure. UltraSurf has gained large popularity among the Internet users, which has daily hits of over 800 million, daily traffic over 8,000 GB, millions of users and users are from over 180 countries.

RESEARCH OBJECTIVES

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

1. To identify how UltraSurf connects to the Internet.
2. To produce strategy to block traffic created by UltraSurf.
3. To evaluate the strategy.

METHODOLOGY

The methodology used seven (7) main phases that were adapted from Peisert & Bishop (2007). This methodology has been used for “How to Design Computer Security Experiment”. In this study two phases were added which are the **“Propose strategy” and the “Validate hypothesis”.** These two phases were added to suite the study that was conducted. Figure 2 shows the methodology used by Peisert and Bishop.

Instead of UltraSurf, Wireshark was used to capture network traffic packet. According to Gerry (2009) and Vasil (2008), Wireshark is the best free tool for protocol analyser. Wireshark has an ability to save captured packet that can be used to analyse later. Figure 3 shows a screen capture of the traffic packet using Wireshark.

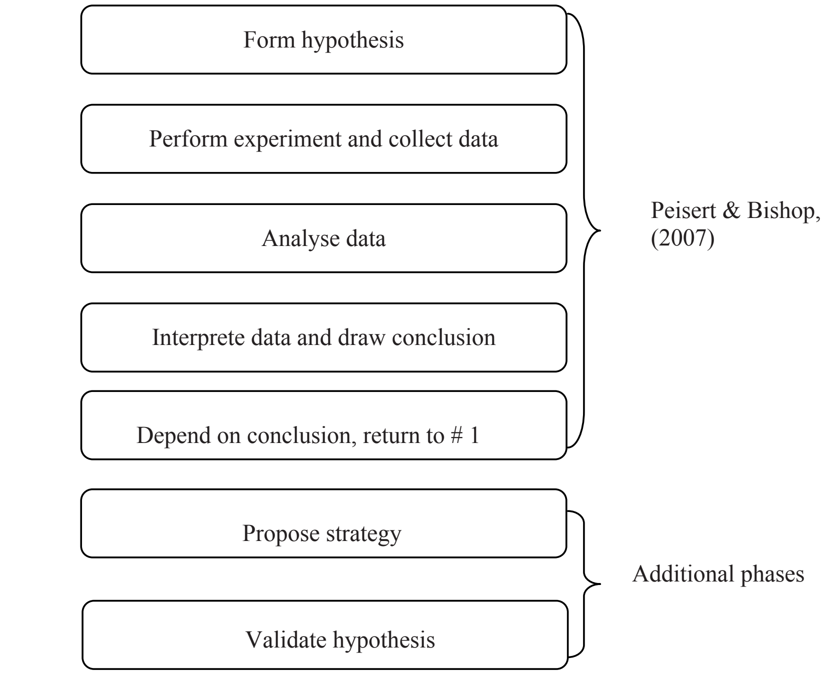
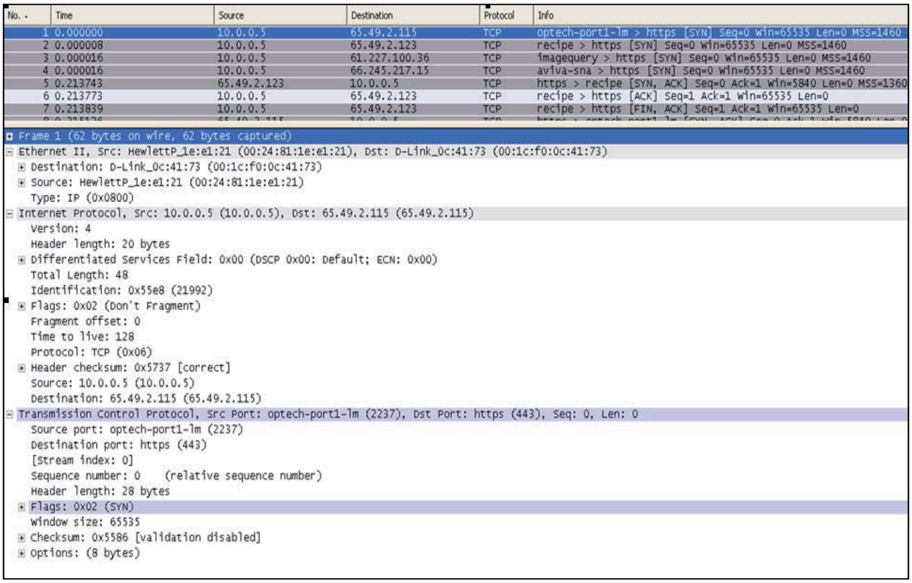

Form hypothesis
Perform experiment and collect data
Analyse data
Interprete data and draw conclusion
Depend on conclusion, return to # 1
Peisert & Bishop, (2007)
Propose strategy
Validate hypothesis
Additional phases

Figure 2. Methodology used in this study.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.5	65.49.2.115	TCP	optech-port1-lm > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460
2	0.000008	10.0.0.5	65.49.2.123	TCP	recipe > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460
3	0.000016	10.0.0.5	61.227.100.36	TCP	imagequery > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460
4	0.000016	10.0.0.5	66.245.217.15	TCP	aviva-sna > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5	0.213743	65.49.2.123	10.0.0.5	TCP	https > recipe [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1360
6	0.213773	10.0.0.5	65.49.2.123	TCP	recipe > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	0.213839	10.0.0.5	65.49.2.123	TCP	recipe > https [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0

```
⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊟ Ethernet II, Src: HewlettP_1e:e1:21 (00:24:81:1e:e1:21), Dst: D-Link_0c:41:73 (00:1c:f0:0c:41:73)
  ⊞ Destination: D-Link_0c:41:73 (00:1c:f0:0c:41:73)
  ⊞ Source: HewlettP_1e:e1:21 (00:24:81:1e:e1:21)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 10.0.0.5 (10.0.0.5), Dst: 65.49.2.115 (65.49.2.115)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 48
    Identification: 0x55e8 (21992)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x5737 [correct]
    Source: 10.0.0.5 (10.0.0.5)
    Destination: 65.49.2.115 (65.49.2.115)
⊟ Transmission Control Protocol, Src Port: optech-port1-lm (2237), Dst Port: https (443), Seq: 0, Len: 0
    Source port: optech-port1-lm (2237)
    Destination port: https (443)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 65535
  ⊞ Checksum: 0x5586 [validation disabled]
  ⊞ Options: (8 bytes)
```

Figure 3. Example of capture data using wireshark.

Wireshark was used to monitor all the lines going to and from a computer and to track where the packet is going. It was used because for sending and receiving replies and also for troubleshooting purposes and optional scenario networks for virtual servers and workstations.

EXPERIMENT AND RESULT

Seven phases were conducted in this study and the result for each phase is explained. The phases were forming hypothesis, performing experiments and collecting data, analysing data, interpreting and drawing conclusions, based on the experiment, proposing strategy and validating the hypothesis.

Phase 1: Form Hypothesis

This phase is forming the hypothesis of this study. The hypothesis information was obtained from the literature review. To identify the requirement for blocking a UltraSurf connection, the processes of web accessing from UltraSurf are listed in Table 1. For each process, the location of the connection and whether the connection can be controlled by the network administrator was identified and labelled as P1, P2, P3 and P4.

Table 1

Process of Connection and the Location it Happened

Label	Process of connection	Location	Ability to control by network admin
P1	Web browser connected to UltraSurf using localhost (ip address 127.0.0.1) port 9666 and created as local proxy server.	Local computer	No
P2	UltraSurf (discovery agent) connected to various external IP (external proxies server) using port https (443) and http (80).	LAN to WAN via Gateway	Yes
P3	External proxies server connected to restricted website and passed back to proxies server.	WAN	No
P4	Proxies server encrypted (if using port 443) the content and sent back to UltraSurf (discovery agent).	WAN to LAN Via Gateway	Yes
P5	UltraSurf as local proxy server passed the content to web browser.	Local Computer	No

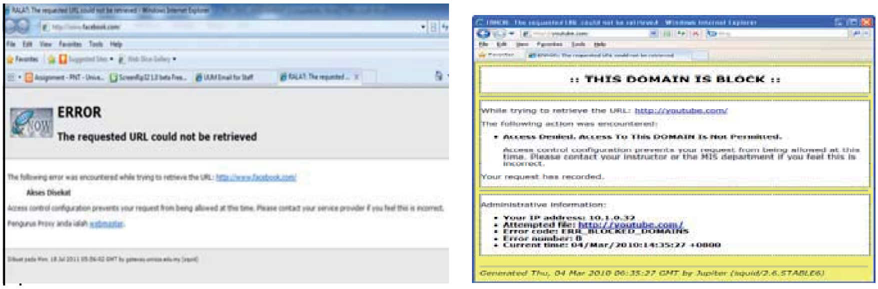
Based on Table 1, the requirement to block UltraSurf was identified in the second process (P2). This process used port https (443) and http (80) and used an organisation gateway to access the Internet. This process happened inside an organisation and under supervision of the network administrator. In a normal organisation a gateway is used to connect to the Internet as it becomes a centre for every computer in LAN. This process is identified as a place to study and conduct an experiment, since it is located in the area where it is controllable and centralized. As an outcome of this phase, a hypothesis "*is it possible to block UltraSurf and how does it connect to the Internet*" ***was identified.***

Phase 2: Perform Experiment and Collect Data.

The second phase carried out the possibilities of creating a simulation to test. This phase was to gather information on how UltraSurf connected the Internet and all the findings was recorded. The experiment was conducted in four (4) conditions and labelled as Exp1, Exp2, Exp3 and Exp4.

Exp1 : Firewall **at router** blocked specific domain name **without** UltraSurf installed.
Exp2 : Firewall **at Squid proxies** blocked specific domain name **without** UltraSurf installed.
Exp3 : Firewall **at router** blocked specific domain name **with** UltraSurf installed.
Exp4 : Firewall **at Squid proxies** blocked specific domain name **with** UltraSurf installed.

All four (4) experiments were tested using 100 domain names for data sampling. The sampling was divided into two sampling domains named "Black List Domain" and "White List Domain". Each sampling contained fifty (50) domain names. The Black List Domain was entered into the firewall to block connection requests from clients. The experiment was done in public and private higher education institution in different locations.


RALAT: The requested URL could not be retrieved - Windows Internet Explorer
http://www.facebook.com/
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
Assignment - PNT - Unive...
ScreenRip32 1.3 beta Free...
UUM Email for Staff
RALAT: The requested...

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://www.facebook.com/

Akses Disekat

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Pengurus Proxy anda ialah webmaster.

Dibuat pada Mon, 18 Jul 2011 05:06:02 GMT by gateway.uniza.edu.my (squid)

ERROR: The requested URL could not be retrieved - Windows Internet Explorer
http://youtube.com
File Edit View Favorites Tools Help
Favorites
ERROR: The requested URL could not be retrieved

:: THIS DOMAIN IS BLOCK ::

While trying to retrieve the URL: http://youtube.com/

The following action was encountered:

- Access Denied, Access To This DOMAIN Is Not Permitted.

  Access control configuration prevents your request from being allowed at this time. Please contact your instructor or the MIS department if you feel this is incorrect.

Your request has recorded.

Administrative information:

- Your IP address: 10.1.0.32
- Attempted file: http://youtube.com/
- Error code: ERR_BLOCKED_DOMAINS
- Error number: 8
- Current time: 04/Mar/2010:14:35:27 +0800

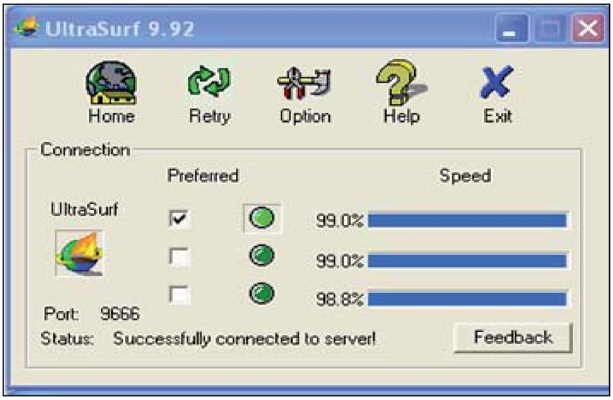
Generated Thu, 04 Mar 2010 06:35:27 GMT by Jupiter (squid/2.6.STABLE6)

Figure 4. A browser message block a blacklist domain.

Figure 4 shows a message from a browser that blocked a Facebook and YouTube websites (blacklist websites). This website data was accessed in different locations without UltraSurf installed.

Phase 3. Analyse Data.

In this phase, the result of each experiment was captured and is shown in Table 2. Figure 5 shows that the Black List Domain (facebook.com) could be accessed with UltraSurf installed although it was blocked by the firewall before the proposed strategy was applied.



Preferred		Speed
☑	●	99.0%
□	●	99.0%
□	●	98.8%

Port: 9666

Status: Successfully connected to server!

Figure 5. Successful connection using UltraSurf.

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

Table 2 shows that in Exp3 and Exp4 those clients installed with UltraSurf were able to access the Black List Domain. It means that the connection through UltraSulf could bypass the firewall either by filtering at the router or the proxy. During Exp3 and Exp4, Wireshark software was used to capture the packet that transmited and received data at the client site. This provided data that could be used in future. Various versions of UltraSurf were used in order to get accurate data. Table 3 shows the summary of the data captured by Wireshark in Exp3 and Exp4 using different versions of UltraSurf.

Table 3

Summary of Packet in Exp3 and Exp4 using Different Versions of UltraSurf

No	Version	Discovery agent in UltraSurf trying to connect using	
		Port	External Proxies IP address
1	9.4	80 and 443	199.67.185.130, 63.245.209.72, 192.88.209.56, 128.231.86.79, 59.106.108.86, 209.85.171.115, 210.59.144.3, 91.192.128.34
2	9.5	80 and 443	65.49.2.115, 65.49.2.123, 61.227.100.36, 66.245.217.15 65.49.2.123
3	9.9.2	443	65.49.2.113, 65.49.2.121, 61.228.183.115, 202.142.160.148, 122.122.159.213, 118.160.154.132

The result shows that UltraSurf used many external proxies IP address in order to bypass the local firewall. These proxies are impossible to be configured manually (using IP address) by the network administrator since UltraSurf will connect with various external proxies to bypass the firewall. It also shows that different versions of UltraSurf were connected to different external proxies.

Phase 4: Interpret and Draw Conclusion

In this phase, it was proved that it was possible to block traffic created by UltraSurf as shown in the previous phase. The connection used http and https ports to communicate with outside servers and UltraSurf used various IP that became UltraSurf external proxies. This phase suggests that blocking communication through IP, will block UltraSurf connection. In this phase Objective 1 “To identify how UltraSurf connects to the internet” has been achieved.

Phase 5: Conclusion based on the Experiment

Based on the outcome of phase 4, a conclusion can be drawn. It supports and agrees with the hypothesis of this study. The analysis of the captured packet in Table 3 shows that:

1. UltraSurf is connected to various external IP addresses.
2. The connection used port 80 (http) and port 443 (https).
3. It used TCP protocol for communication.

The results also shows that different versions of UltraSurf are connected to different external proxy IP addresses. For example, UltraSurf version 9.4 was connected to a different external proxy IP address which was impossible for the network administrator to block the various IP address.

Phase 6: Propose Strategy

Based on the result of the experiment, this phase exposes a strategy on how to filter and block UltraSurf. All the captured packet generated by Wireshark was analysed. As an outcome from the previous phase, one strategy has been established which is: "To reject ALL traffic using TCP protocol port 80 and port 443 that try to connect based on IP address". This is shown in Figure 6. The client PC installed with or without UltraSurf would access the Internet through the router or the firewall. The Black List Domain was rejected at the router/firewall and tried to access through the Squid proxy via port 80/443. However, by using the proposed system, all Black List Domains were rejected at the Squid proxy level. This is because UltraSurf was encrypting the domain to an IP address. This IP address was rejected by the Squid proxy that blocked all http using the IP address.

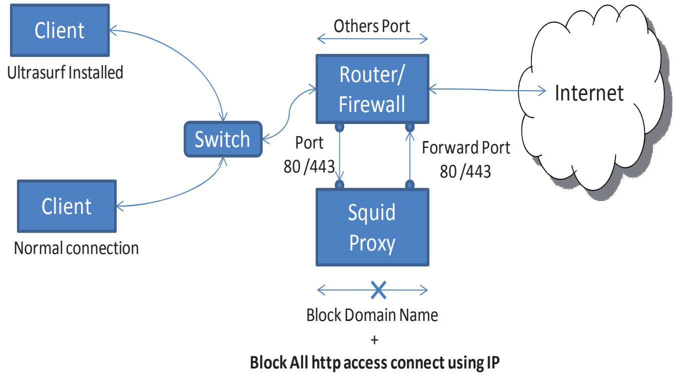


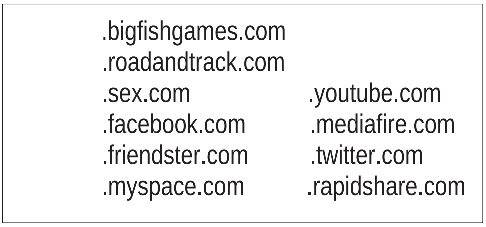
Figure 6. Proposed system.

Tables 3 shows UltraSurf using port 80 and 443 to bypass the firewall. Exp3 and Exp4 also show that clients installed with UltraSurf are able to bypass the router firewall and the proxies firewall. In order to block the restricted website, the server in Squid proxy server was configured as follows:

```
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
```

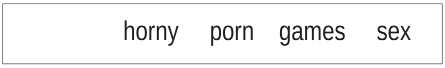
Figure 7. Squid.conf.

In Figure 7, the important 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 the users that try to access http and https using the IP address as URL.



```
.bigfishgames.com
.roadandtrack.com
.sex.com             .youtube.com
.facebook.com        .mediafire.com
.friendster.com      .twitter.com
.myspace.com         .rapidshare.com
```

Figure 8. Blacklist_domains.acl.



```
horny   porn   games   sex
```

Figure 9. Blacklist_domains_contain.acl.

Figure 8 and Figure 9 show additional files to support squid to block specific domains and any domain containing specific words in their domain names. In this phase objective 2 “To produce a strategy that is able to block UltraSurf” **has been achieved.**

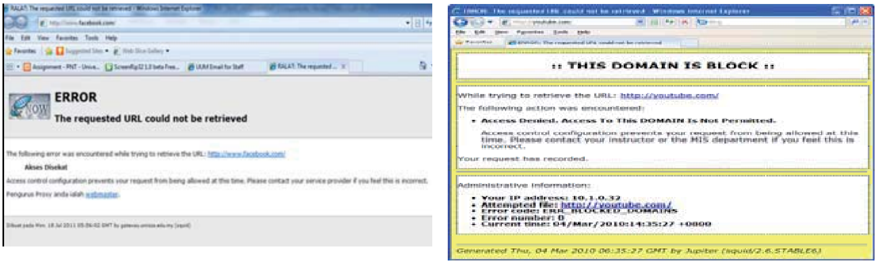
Phase 7: Validate the Hypothesis

In this phase, the strategy has been applied into an organisation firewall and the effect has been analysed to prove whether the strategy is working or not. Based on the proposed strategy, Exp4 (web filtering at squid with UltraSurf installed) was conducted again to validate the requirement needed as shown in Table 4. Experiment 3 was not conducted in this study due to a few constraints. However it will be continued in the next study.

Table 4

Validate Result

Domain Name	Exp1	Exp2	Exp3	Exp4
White List Domain	Yes	Yes	-	Yes
Black List Domain	No	No	-	No



RALAT: The requested URL could not be retrieved - Windows Internet Explorer

http://www.facebook.com/

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: http://www.facebook.com/

Akses Disekat

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Pengurus Proxy anda ialah webmaster.

Dibuat pada Mon, 18 Jul 2011 05:06:02 GMT by gateway.unisza.edu.my (squid)

ERROR: The requested URL could not be retrieved - Windows Internet Explorer

:: THIS DOMAIN IS BLOCK ::

While trying to retrieve the URL: http://youtube.com/

The following action was encountered:

- **Access Denied. Access To This DOMAIN Is Not Permitted.**

  Access control configuration prevents your request from being allowed at this time. Please contact your instructor or the MIS department if you feel this is incorrect.

Your request has recorded.

Administrative information:

- **Your IP address: 10.1.0.32**
- **Attempted file: http://youtube.com/**
- **Error code: ERR_BLOCKED_DOMAINS**
- **Error number: 0**
- **Current time: 04/Mar/2010:14:35:27 +0800**

Generated Thu, 04 Mar 2010 06:35:27 GMT by Jupiter (squid/2.6.STABLE6)

Figure 10. UltraSurf unable to connect to Internet.

Figure 10 shows that UltraSurf is unable to connect to the external IP after the proposed acl configuration has been applied. All White List and Black List Domains cannot be accessed by users even though UltraSurf was installed in their PCs. This shows that a user PC installed with UltraSurf is unable to access the Internet. Since this strategy cannot be applied inside the router firewall, Experiment 3 was not conducted.

Table 5

The Result Before and After Implement the Proposed Strategy (with UltraSurf installed)

	Before configuring the proposed strategy			After configuring the proposed strategy		
Domain Name	Exp1	Exp2	Exp4	Exp1	Exp2	Exp4
White List	√	√	√	√	√	√
Black List	√	√	√	χ	χ	χ

√ can access the website χ cannot access the website

Table 5 shows the result before and after configuring the proposed strategy with UltraSurf installed. The entire Black List Domain cannot be accessed by the user although the user PC was installed with UltraSurf.

CONCLUSION

While the experiment was conducted, most of the firewall was unable to block anti-censorship software such as UltraSurf. A strategy to combat anti-censorship should be introduced to protect the organization. This project has introduced a strategy to block users from accessing prohibited websites. Squid proxy server has an ability to provide a blocking IP address based on the http and https connections. Based on this study two techniques of implementation are proposed as shown in Figures 11 and 12.

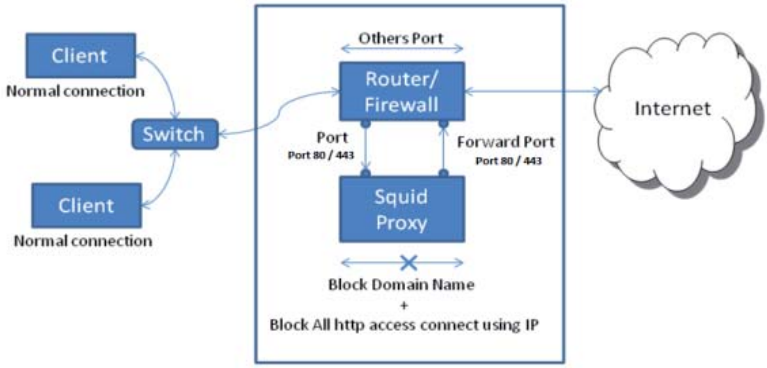


Figure11. Router, firewall and proxy in a box.

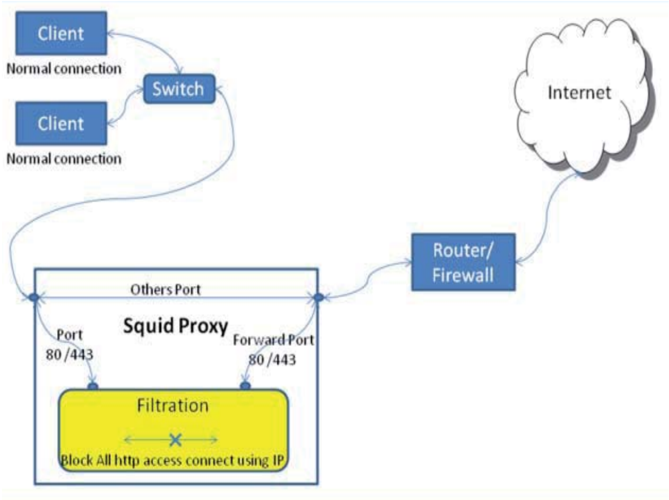


Figure 12. Independent proxy.

Figure 11 shows the strategy to implement restriction in accessing the website in a single box. This box acts as the router/firewall and proxies. Figure 12 is proposed since this strategy used squid to filter and block the restricted website. Based on Experiment 3 (firewall at router blocked specific domain name with UltraSurf installed). This strategy cannot be applied directly in a router or a firewall. However, as shown in Figure 12, this strategy was applied outside a router/firewall to filter and block UltraSurf. The key for this strategy is "To reject ALL traffic using TCP protocol port 80 and 443 that try to connect based on IP address". This means if a user tries to connect to the Internet using http or https he/she must use the domain name. If the user uses the IP address, Squid will drop this network traffic request. Squid is also able to configure whether to allow connections using specific IP addresses. Squid as proxy's server plays a vital role in this strategy.

FUTURE DEVELOPMENTS

This strategy of blocking UltraSurf traffic requests can be enhanced in many ways and there will always be new developments evolved in this anti-censorship technology. This reveals the new areas for researchers to explore. The following entries will briefly present further enhanced specifications such as performance, Squid new technology, Network mode and other types of anti-censorship software.

i. Performance.
This research study did not touch on performance to process the filtering traffic request. For example, what would happen if 1000 users requested at the same time. Is the Squid server able to support and what is the best hardware specification to handle connections efficiently?

ii. Squid new technology.
The Squid proxy servers keep updating their features to meet the users' targets. The question Are current squid configurations (Squid.conf) working perfectly in all versions of squid need to be answered.

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

iv. Others types of anti-censorship software
As mentioned in Chapter 1, there are many anti-censorship software available in the market. The software are UltraSurf, Freegate, Gpass, GTunnel and FirePhoenix. In these study only UltraSurf has been tested. The same strategy may work on other anti-censorship software as well.

REFERENCES

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

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

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

Danyaro, K. U., Jaafar, J., De Lara, R. A. A., Downe, A. G.(2010). An evaluation of the usage of Web 2.0 among tertiary level students in Malaysia. *IEEE Conference Information Technology (ITSim), International Symposium in GIFC.*

Hunter, C. D. (2000). Internet filter effectiveness (student paper panel): Testing over and under inclusive 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). Technopedia. Retrieved 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. (2006, December). 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. (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 from Sample Regular Expressions: http://www.regular-expressions.info/examples.html

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

Strange Maps. (2007). A map of the internet's black holes. Retrieved from 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.

Watt, A. (2005). *Beginning regular expressions.* John Wiley & Sons.

Xia, B. (2004). The coming crash of the matrix. *China Right Forum*, 42-44.