STRATEGY TO FILTER AND BLOCKING TRAFFIC CREATE BY ANTI-CENSORSHIP SOFTWARE IN LOCAL AREA NETWORK

A thesis submitted to the Graduate School in partial
fulfillment of the requirement for the degree
Master Of Science (Information Technology)
Universiti Utara Malaysia

By

Kamal Harmoni Kamal Ariff
2010

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

KAMAL HARMONI KAMAL ARIFF
(801584)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

STRATEGY TO FILTER AND BLOCKING TRAFFIC CREATE BY ANTI-CENSORSHIP SOFTWARE IN LOCAL AREA NETWORK

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **MR. ALI YUSNY DAUD**

Tandatangan
(Signature) : 

Tarikh
(Date) : 9/5/2010

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRACT

Anti-censorship software originally develop to fight internet censorship in China. The anti-censorship software such as Ultrasurf, Freegate, Gpass, GTunnel and FirePhoenix are become popular for the user who used the internet for thier own's purpose and disobey the policies. 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.

ABSTRAK

Perisian anti-penapisan dibangunkan bagi menyekat proses penapisan internet yang dijalankan di China. Perisian anti-penapisan tersebut adalah seperti UltraSurf, FreeGate, GPass, GTunnel dan FirePhoenix menjadi terkenal kepada penguna yang mengunakan intenet bagi kegunaan mereka sendiri dan juga tidak mematuhi polisi internet. Semenjak itu, perisian ini mula digunakan secara meluas oleh penguna sistem rangkaian dalaman "LAN" dalam sebuah organisasi untuk menembusi polisi "Firewall". Hal ini menjadi ancaman kepada pihak yang mentabir polisi internet dalam sesebuah "LAN" dan juga kepada penggunaan internet biasa. Bagi sesebuah organisasi keadaan yang tidak terkawal ini menyebabkan sistem rangkaian dalaman terdedah kepada ancaman virus, "backdoor", aktiviti tidak produktif dan memperlahankan kelajuan rangkaian itu sendiri. Oleh itu, tujuan penyelidikan ini dibangunkan untuk mewujudkan strategi untuk menapis dan mengekang aktiviti anti penapisan yang berleluasa di dalam sistem rangkaian dalaman "LAN". Projek ini dijalankan menggunakan metadologi "design computer security experiment". Oleh yang demikian, tujuan projek ini dijalankan bagi membantu pentabir sistem rangkaian, untuk mengawal kepenggunaan internet, melindungi dan membenarkan perlaksanaan polisi internet di dalam sesebuah organisasi dipatuhi.

Specially dedicated to…… anis, hidayah and hidayat
for encouraged and guided me throughout my journey of education
and lastly to all Open Source Community.

ACKNOWLEDGEMENTS

First and foremost, let me be thankful and grateful to the Almighty Allah SWT, the Creator and Sustainer of this whole universe, the Most Beneficent and the Most Merciful for His guidance and blessings, and for granting me knowledge, patience me and perseverance to accomplish this research successfully.

I would like to express my sincere gratitude to En. Ali Yusny for advising me during the development of this project and keeping the project focused and directed.

To KISMEC staff for conduct simulation, testing and implementing this studies. Especially to Nuraini, Rahman, Raduan and KISMEC student for their involvement during evaluate of this project.

Finally, I would also like to thank my wife Anisah Ahmad for her patience and support during the development of the studies.

April 2010,
Kamal Harmoni Kamal Ariff

Table Of Content

LIST OF TABLES

LIST OF FIGURES

-- Intentionally Blank --

CHAPTER 1

INTRODUCTION

1.1 Overview

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

The contents of the thesis is for internal user only

BIBLIOGRAPHY

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.

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