UNIVERSITI TEKNOLOGI MARA

AN IMPLEMENTATION OF OPEN SYSTEMS INTERCONNECTION (OSI) TRANSPORT LAYER P2P IDENTIFICATION ALGORITHM USING NETFLOW AND NETFILTER AS P2P TRAFFIC FIREWALL

AMIR HERMAN BIN AMIRUDDIN

Dissertation submitted in partial fulfillment of the requirements

for the degree of

Master of Science in Computer Networking

Faculty of Computer and Mathematical Sciences

January 2014

ABSTRACT

Popularity of P2P applications usage; majorly on file-sharing and video streaming has gained vast popularity and so rapid which wake up network service providers of its dominance. With the ability of P2P network connecting multiple clients with other multiple clients, P2P traffic tends to occupy and congest a bandwidth pipeline. Most of the industry's P2P bandwidth management solutions adopted Deep Packet Inspection (DPI) method for high traffic controlling accuracy. However, this approach has its setbacks which are (i) Traffic Bottleneck (ii) Extensive Resources and (iii) Encrypted Payload. The purpose of this dissertation was to implement OSI Transport Layer P2P identification algorithm using Netflow and Netfilter as a P2P traffic firewall. Using a novel firewall framework designed in this dissertation, an algorithm adapted from research by Yan, Wu, Luo, & Zhang (2013) was used for the P2P identification method. Tested on a university WiFi campus network to measure (i) P2P Identification Ability, (ii) Firewall Hardware Resources and (iii) Number of firewall rules, the Netflow data of its traffic were processed to detect any possible P2P host. The ability of detecting P2P host by this algorithm was compared to the detection rate of operational DPI appliances in the network. The experiment showed that, for P2P identification ability, Netflow based algorithm detected 28.7% more than DPI. Further investigation clearly showed it was because DPI failed to detect encrypted P2P hosts compared to DPI. The result also showed over a period of 60 hours; the firewall server utilizes in average of 4% to 5% of CPU and 5.08 Gb from total 8.0 GB respectively. The number of firewall rules created was average at 456.70 for every each 10 minutes cycle over a sampling of 60 hours. This research has proved that it is capable of detecting P2P traffic with higher accuracy in comparing to DPI method, utilized low resources and capable in creating P2P hosts blocking firewall rules thus proved the P2P firewall framework solution design to be valid and implementable in a real network. For future works, it was recommended to explore new heuristics P2P identification using IPFIX which will commission to become a future network flow standard by IETF.

ACKNOWLEDGEMENT

In the name of ALLAH the most beneficent the most merciful.

Praise to ALLAH for giving me HIS 'hidayah' and blessing.

Deepest gratitude to my supervisor En Farok Hj Azmat and examiner Dr Tn Hj Mohd Izani Mohamed Rawi for their valuable guidance and encouragement throughout the completeness of this dissertation.

To Ayah and Mak, thank you for giving me your 'doa', support and believe on me to continue my education journey. My beloved wife Sharipah Ahmad…thanks for always being there with me. There is no word to describe how grateful I am to have someone like you in my life. To Nur Sofiyyah and Amir Hibban, thanks for being a wonderful kids and cherish up your daddy's life. You are my the truly inspirational and motivational jewels.

Lastly my sincere thanks to my big family, fellow coursemate of CS778 (you guys are the best), CS778 lectures (Thanks for sharing your knowledge. I learned so much), colleagues at JARING, the Inner Circle (you know who you are), Adzmely (for lending me his server), my 'sedulur' (jazaakumullahu kghoiroo) and each person who directly and indirectly lent their helping hand and doa in this wonderful venture.

THANK YOU

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Overview

The main focus of this research paper is to design, develop as well as analyze a Peer-to-Peer (P2P) firewall based on Netflow. This chapter serves as an introductory to explain the background of the study. Information from the background will then direct to the problem statement which this paper intends to solve. It also presents the objectives and significance of the research. Finally, this chapter will describe the whole structure and organization of this dissertation.

1.1 Background of Study

In the evolution of internet technologies and its usages, internet has been the carrier of multiple packets services mainly goes to data, voice and images. In the infant age of the internet, web browsing dominates the majority of the traffic flow. However, since 1999 when P2P firstly emerged, it shockingly shifted the traffic trend from web traffic dominated to file sharing. In time, the popularity of P2P applications usage; majorly on file-sharing and video streaming has gained vast popularity and so rapid which wake up network service providers of its dominance. It is estimated that currently up to 90 percent of local and 60 percent of backbone traffic is P2P traffic(Mellin, 2004).