An Analysis of Network Activity in a Public University

Rozano S. Maniaol
Institute of Computer Science
University of the Philippines Los Banos
rsmaniaol@up.edu.ph

Danilo J. Mercado
Institute of Computer Science
University of the Philippines Los Banos
djmercado@up.edu.ph

ABSTRACT

This paper presents the evaluation of the network activity of a public university using a report generated by the campus network firewall appliance. The results were taken by monitoring the network activity of about 18,000 students, faculty, and staff using various IP data network services such as Web, VoIP, Video Conferencing, CCTV and others. Understanding the usage patterns, security attacks and threats are essential for planning, securing and maintaining the campus data network. A policy recommendation was crafted based on the results of the analysis.

Keywords

campus network; traffic analysis; next-generation firewall

1. INTRODUCTION

Information and Communication Technology is a necessary enabling factor in learning and research [1]. Global collaboration among teachers, students and researchers can now be easily done through Internet applications such as email, video streaming, online chats, and virtual learning environments [2]. However, in the Philippines, Internet infrastructure and bandwidth is very expensive [3] and thus must be properly managed to ensure efficient utilization.

Analyzing the network activity to understand the behavior and usage of internet users contributes to capacity planning and provisioning, anomaly finding, traffic engineering, costing, fault diagnosis, and application performance [4]. It guides university administrators particularly IT officers to develop IT strategic plans and policies that adheres to the university's vision and mission. In addition, public institutions have budgetary constraints [5] that the efficient use and allocation of resources are factors in these plans and policies. A research university would certainly disapprove the use majority of its internet bandwidth for social media, video streaming or file sharing which are not related to its academics. These activities may divert its resources to other concerns like increasing subscription and access to online journals and courses. Understanding how students, faculty and staff use internet bandwidth helps in the selection of the appropriate network equipment or possibly in the redesign of the network architecture for expansion [6]. Likewise, knowledge of the threats of the network prepares system and network administrators for the needed protection and recovery procedures of important data. Today, reliable, scalable and secure connections are necessary considerations of network design [7]. Delivering data when and where they are needed justifies the procurement of essential equipment, additional bandwidth and policy recommendations.

This paper presents internet traffic data collected by a next-generation firewall appliance. Network activity logs were captured for eight weeks. Data showed the top applications used, the top hosts that initiated the network activity and their location, the top destination countries, the top blocked threats and host that visited malicious sites. Further analysis was done by categorizing the users. Host IP addresses were linked with inside campus subnetworks. These subnetworks were then clustered based on the university academic and administrative functions to determine the top users of bandwidth in campus.

The result of this study is a policy recommendation based on the network traffic and common threats encountered. The purpose of this policy is to correct the usage of Internet bandwidth and protect the users and their data from malicious attacks.

2. RELATED WORK

Several studies on campus network analysis were done differing in focus and methods on their evaluation of the network traffic.

Ibrahim [8] analyzed Universiti Utara Malaysia's internet traffic based on users' preferences. They gathered their data by port mirroring the main distribution switch and filtering the results using Wireshark[1] to isolate HTTP packets. The results indicated that the three largest traffic came from social networking sites, search engines and E-commerce sites with 42%, 19% and 9% respectively. The study recommended limiting access to social network and video streaming sites during working or studying hours.

Waheed [9] gathered the King Fahd University of Petroleum and Mineral campus web proxy server logs for one month and validated the well-known Web traffic characteristics in terms of website popularity and type of content. Most visited sites were in North America which added excessive de-

[1]https://www.wireshark.org