A PROPOSED NETWORK SECURITY MECHANISM FOR ISPSC STA.MARIA CAMPUS

ARDENNE LEI DOMINGO

CRISOSTOMO PERALTA

EDWARD DASALLA

MARVIN DAPROZA

CHERRY JOY LAYA

MAY DANO

A CAPSTONE PROJECT PROPOSAL PRESENTED TO THE FACULTY OF

THE ILOCOS SUR POLYTECHNIC STATE COLLEGE

INSTITUTE OF COMPUTING STUDIES

STA.MARIA CAMPUS

BACHELOR IN INFORMATION TECHNOLOGY

MAY 2017

TABLE OF CONTENTS

PRELIMINARIES		PAGES
	Approval Sheet	i
	Acknowledgement	ii
	Dedication	v
	Executive Summary	ix
	Table of Contents	xii
CHAPTER		
I	**INTRODUCTION**	
	Project Context	1
	Purpose and Description	5
	Objectives of the Project	6
	Scope and Limitation	
II	**REVIEW OF RELATED LITERATURE**	7
III	**TECHNICAL BACKGROUND**	14
	Performance Analysis	15
	Security Analysis	15
IV	**METHODOLOGY**	16
	Project Staff and Functions	17
	Data Gathering Procedures	18
	Sources of Data	19
V	**RESULTS AND DISCUSSION**	23

VI SUMMARY, CONCLUSION AND RECOMMENDATION 29

BIBLIOGRAPHY 33

APPENDICES 34

Chapter I

INTRODUCTION

Project Context

The concept of having an institution or organization network as an isolated LAN is no longer applicable. Everyone wants to be online and have Internet access. This accessibility is intriguing to attackers with malicious intentions to breach the network and access its assets. Attempting to protect workstations individually is not practical. A better solution is to use a firewall to isolate the LAN from the Internet and examine all the traffic going in and out of the network.

The integration between intranet and the Internet requires a secure gatekeeper to protect against network-based security attacks. Firewalls usually protect the network from such threats while continuing to allow information exchange with the outside world. Hence, defining a firewall as a device providing a perimeter security is not a valid definition. Although system administrators work to enforce their network traffic to pass through the firewall, some internal users continue to have an Internet connection that bypasses the firewall.

A firewall must guarantee that only authorized users access an operating system or a computer connected to a

network, securing by that private information and defending computer users from identity theft. In most cases, firewalls block unauthorized access that computer users are not aware of.

Firewalls are categorized into two main types: network-based and personal. A network-based firewall is usually installed at the edge of the network connecting the LAN with the broadband access. A personal firewall, also known as desktop or software firewall, is a program that is installed on personal devices (e.g., laptop) similar in that to an antivirus. In most cases, system administrators install both types of firewalls in order to protect against attacks that bypass network-based firewalls and to provide layered security.

In computer network systems, only general and multilayered security infrastructure can manage with the possible attacks. This paper presents security mechanisms on application, transport and network layers of ISO/OSI reference model and gives examples of the today most popular security protocols applied in each of the mentioned layers (e.g. S/MIME, SSL and IPSec). We recommend a secure computer network systems that consists of combined security mechanisms on three different ISO/OSI reference model layers: application layer security (end-to-end security) based

on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards), transport layer security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure and network IP layer security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks. These layers are projected in a way that a vulnerability of the one layer could not compromise the other layers and thus the whole system is not vulnerable. User strong authentication procedures based on digital certificates and Public Key Infrastructure (PKI) systems are especially emphasized.

Little work is done on assessing the impact of firewalls on network performance and their resilience against security attacks. Since a common concern of network users is the efficiency of the used firewalls, in this paper we present an assessment methodology to analyze the performance of different firewalls platforms. The performance analysis considers delay, jitter, throughput, and packet loss. The security of firewalls is also tested by applying a set of attacks and observing the reaction of the firewalls. The proposed methodology is tested by performing real experiments on

different types of firewalls including those that are personal and network-based.

Today Firewalls have become the staple of network security architectures, primarily providing access control to network resources, and they have been successfully deployed in the large majority of networks like government organization and individual users. Firewall and Intrusion Detection (IDS) are adopted more frequently. Network attacks a crucial element in providing networks with the reliability required in today's competitive environment. However, while most firewalls provide effective access control, many are not designed to detect an attacks at the application level.

Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, decryption and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection system started appearing in the last few years. Using intrusion detection system, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected can be used to hardening your network security, and legal purposes. The Internet is a network of computer networks. It has evolved from the interconnection of networks around the globe. Internet connection may be used by "hackers" (or as some would rather call them "crackers") to gain

unauthorized access to your local network. Availability of computing facilities can also be targeted by Denial of Service (DoS) attacks. So the comparison of different types of firewalls and IDS are required for providing security to networks.

Moreover, computers became convenient in every household, company, educational institution, entertainment venue, and other public areas. Most of the users are non-professionals including students, employees, children, and other users. This means that most users have little knowledge on network security, if any. Therefore, a secondary objective of this paper is to explore the level of knowledge of a sample of college students on the importance of fire- wall and their usage. To study this issue and the aforementioned objective a quantitative study was conducted and the results and conclusions are illustrated in this paper.

Purpose and Description

Network Administrators. The output of the study will provide a better view of network security for ISPSC.

Students. The students will understand the idea of having a good network security to avoid threat or harm in the internal network of the campus.

Researchers. This research paper will help the researchers enhance their knowledge in computer network security.

Future Researchers. The study would help future researchers the further understand the setup of having a secured computer network and might enhance this paper in future based on new security trends.

Statement of Objectives

This capstone project aims to test the performance and security feature of the network-based firewall to be used for an enhanced network security mechanism for ISPSC Santa Maria Campus. Specifically the study aims to:

1. To identify the network security infrastructure setup of ISPSC Santa Maria Campus;
2. To test the performance and security of firewalls to be used for ISPSC;
3. To recommend to establish a network firewall for ISPSC Santa Maria Campus.

Scope and Limitation

The scope of the study will focus in applicable firewall to be used for ISPSC Santa Maria Campus that will serve as a mechanism to prevent the computer network of ISPSC Santa Maria from threat or malicious infections. The identified security firewall will be the tool to prevent threats in all of the computers in the campus.

The security mechanism will not only be limited on the implementation on a Microsoft Windows Environment but it may also be applied in other types of Operating System.

Chapter II

REVIEW OF LITERATURE

Little work was published on firewall performance analysis. Most of the available work considered enhancing firewalls configuration management and detecting misconfiguration as presented in research paper references from studies of A. El-Atawy et. al (2007), Lihua Yuan et. al. (2006), A.X Liu and M.G Gouda (2008), G. Misherghi et. Al (2008) and Mohamed G. Gouda and Alex X. Liu (2007).

Salah et al. (2012) studied the performance of firewalls using analytical queuing model based on Markov chain. The methodology analyzes firewalls that are subject to normal traffic flows as well as DoS attack flows.

In a study by C. Sheth and R. Thakker (2011) the researchers examined various types of firewalls operations. They tested the performance and security for various firewalls including: Cisco ASA, packet filter, and Checkpoint SPLAT. In terms of performance, the researchers only considered the through- put and the maximum number of concurrent connections. Their results showed that Cisco ASA provides better performance compared to the other two firewalls. As for security, they performed simple tests and reported that the firewalls demonstrated good resistance.

In a research of S. Nassar et. Al (2010) the researchers studied the effect of implementing a firewall on the network performance. Their simulation results showed that using firewalls increases the network delay and average response time. Moreover, they suggested using parallel firewalls to improve the network performance. Researchers in the study of M.Z.A. Aziz et. Al (2012) investigated the performance of application layer firewalls in terms of response time and link utilization. The simulation results proved that firewalls degrade the performance of the network. The researchers experimentally evaluated and modeled Linux kernel firewalls focusing on the error-caused security vulnerabilities and resulting security violations. In a research of Collin Jackson et. Al (2009) showed that using DNS rebinding can circumvent firewalls and disrupt an intranet. They proposed the use of a personal tool called dnswall to combat firewalls circumvent.

In summary, none of the previous work presented a comprehensive analysis on the impact of firewalls on the network performance. Therefore, this paper aimed to compare network-based and host-based firewalls in terms of performance and security.

A firewall can be defined as an electronic device or program that manages the flow of data and information that are going in

or out of a network. The aim is to prevent unauthorized access to the network from an adversary which could lead to data loss and exploitation of the services. In computer networks, firewalls are the gatekeeper of the network that examines all incoming and outgoing data packets to determine whether they are authorized or not based on a set of predefined rules.

The idea of firewalls is to construct a bridge between an internal private network and system (that is assumed to be secure and trusted), and the outside world (i.e., the Internet which is public, untrusted, and contain adversaries).

Firewalls are roughly classified into personal and network based firewalls (William Stallings, 2011). Personal or also called "host-based" firewalls are usually software applications that are installed to run on the operating system. Nowadays, most of the operating systems come with a built-in firewalls. Personal firewalls are becoming very popular and they aim to protect individual hosts from malicious packets by performing host packet filtering. While network- based firewalls are available, one would question the need of personal firewalls. Moreover, personal firewalls are the best, if not the only, option for mobile users. In addition, they protect against connections that bypass the network firewall to form a layered defense. In personal computers, firewalls test whether an installed software is

allowed to access the Internet, performing by that what is known as egress filtering.

Network-based firewalls consist of: hardware, software, and firmware that are particularly optimized for firewall functionality. This makes them capable of providing a higher performance compared to personal firewalls. Other advantages include:

1. Simplifying security management
2. Facilitating implementation of advanced logging and monitoring
3. Allowing creation of a VPN using IPSec to other hosts
4. Enabling segmentation and isolation of problems
5. Hiding the IP addresses of client stations in an internal network by presenting one IP address to the outside world

On the other hand, disadvantages of network based firewalls include being a bottleneck and a possible single point of failure. This strictly requires firewalls to be as tamper proof as possible and to operate with high efficiency to avoid degrading the network performance. Figure 1 shows the main types of firewalls (William Stalling, 2011).

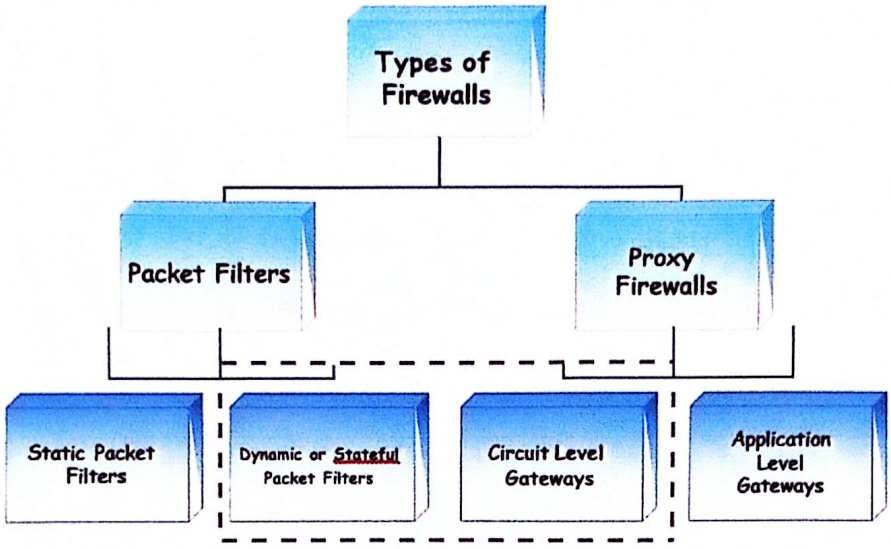

Figure 1. Types of Firewalls

Packet filtering firewalls are the simplest firewalls which is mostly a router that has capability to filter packets. They typically work on layer three and layer four of the OSI model. Packet filtering rules are defined to match the packets and determine which traffic is allowed or denied. The main advantage of packet filtering firewalls is their simplicity and capability to quickly process packets in order to provide protection against attacks. Despite the advantages of packet filters they cannot prevent application layer attacks and are susceptible to certain types of TCP/IP protocol attacks.

Stateful firewalls are more intelligent than packet filters as they examine the state of a connection when data being initiated, transferred or terminated. A stateful firewall examine information in the packet header of layer 3 and layer 4. For

example, it looks at the TCP header for SYN, RST, ACK, and FIN to determine the state of the connection. The stateful firewalls can detect the state of the connection and can prevent some types of DOS attacks. Generally, stateful firewalls are used as an intelligent first line of defense without adding extra cost. However, they cannot prevent application layer attacks and may cost an additional overhead in maintaining a state table.

Proxy firewalls, unlike other firewalls, they reproduce application layer functionality where packets are not examined individually but rather collectively decoded instead. Examination after decoding usually indicates whether or not the packets belong to a valid request. Proxy firewalls, also known as gateways, act as a relay for applications. The users in a LAN contacts the proxy with identification information. Then, the proxy acts on the behalf of the user and contacts the application server. Afterwards, it relays packets between the user and the application server while shielding either side from direct connection.

The proxy needs to be configured for each service (e.g. e-mail, web, FTP) the administrator wants to provide in the network. Proxies provide a deeper traffic examination and consequently deliver higher levels of security. However, this

advanced level of security compromises the network performance network in terms of delay, jitter, and throughput. Another drawback of using a proxy is that disturbing it causes the entire network to mal- function. Attackers are usually aware of this vulnerability which makes proxies an obvious target.

BIBLIOGRAPHY

A. El-Atawy, T. Samak, E. Al-Shaer, and Hong Li. Using online traffic statistical matching for opti- mizing packet filtering performance. In In Proc. of IEEE INFOCOM, pages 866–874, 2007.

Lihua Yuan, Hao Chen, Jianning Mai, Chen-Nee Chuah, Zhendong Su, and P. Mohapatra. Fireman: a toolkit for firewall modeling and analysis. In In Proc. of IEEE Symposium on Security and Privacy, pages 15 pp.–213, 2006.

A.X. Liu and M.G. Gouda. Diverse firewall design. Parallel and Distributed Systems, IEEE Transactions on, 19(9):1237–1251, 2008.

G. Misherghi, Lihua Yuan, Zhendong Su, Chen-Nee Chuah, and Hao Chen. A general framework for benchmarking firewall optimization techniques. IEEE Trans. on Netw. and Serv. Manag., 5(4):227–238, December 2008.

Mohamed G. Gouda and Alex X. Liu. Structured firewall design. Comput. Netw., 51(4):1106–1120, March 2007.

K. Salah, K. Elbadawi, and R. Boutaba. Performance modeling and analysis of network firewalls. IEEE Transactions on Network and Service Management, 9(1):12–21, 2012.

C. Sheth and R. Thakker. Performance evaluation and comparative analysis of network firewalls. In In Proc. of IEEE ICDeCom, pages 1–5, 2011.

S. Nassar, A. El-Sayed, and N. Aiad. Improve the network performance by using parallel firewalls. In Proc. of IEEE INC, pages 1–5, 2010.

M.Z.A. Aziz, M.Y. Ibrahim, A.M. Omar, R. Ab Rahman, M.M. Md Zan, and M.I. Yusof. Performance analysis of application layer firewall. In In Proc. of IEEE ISWTA, pages 182–186, 2012.

Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting browsers from dns rebinding attacks. ACM Trans. Web, 3(1):2:1–2:26, January 2009.

William Stallings. Cryptography and Network Security: Principles and Practice. Pearson Education, 5th edition, 2011.