UNIVERSITI TEKNIKAL MALAYSIA MELAKA

IMPLEMENTATION PARALLEL FIREWALL AT COSMOPOINT MELAKA TO IMPROVE PERFORMANCE

NALIZAWATI BINTI NOH

MASTER OF COMPUTER SCIENCE (INTERNETWORKING TECHNOLOGY)

2017

Faculty of Information and Communication Technology

IMPLEMENTATION PARALLEL FIREWALL AT COSMOPOINT MELAKA TO IMPROVE PERFORMANCE

Nalizawati Binti Noh

Master of Computer Science (Internetworking Technology)

2017

Universiti Teknikal Malaysia Melaka

IMPLEMENTATION PARALLEL FIREWALL AT COSMOPOINT MELAKA TO IMPROVE PERFORMANCE

NALIZAWATI BINTI NOH

A dissertation submitted
in fulfillment of the requirements for the degree of Master of Computer Science
(Internetworking Technology)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I declare that this dissertation entitled "Implementation Parallel Firewall at Cosmopoint Melaka to Improve Performance" is the result of my own research except as cited in the references. The dissertation has not been accepted for any master and is not concurrently submitted in candidature of any other master.

Signature   :   …………………………………..

Name   :   …………………………………..

Date   :   …………………………..………

APPROVAL

I hereby declare that I have read this dissertation and in my opinion this dissertation is sufficient in term of scope and quality for the award of Master of Computer Science (Internetworking Technology).

Signature   :   ……………………………..

Supervisor Name   :   PM Dr Abdul Samad Shibghatullah

Date   :   ………………..…………

DEDICATION

Dedicate with love and affection to my family

Dedicate the dissertation to people who have inspired the researchers while doing the

dissertation.

ABSTRACT

Nowadays, the concept of having isolated LAN for an institution network is no longer relevant. This thing same goes with the Cosmopoint College Melaka. Internet became is an essential part and plays an important role in institution. So, firewall became is an important components in improving network security. It's can examine all the in and out traffic of the network. This dissertation focused on the study about relationship between security and network performance. Its will demonstrate the concept of firewall, function of firewall in the network, the types of firewall and its importance in the network. Besides that, this dissertation will discuss the effect brings to network performance while implementing the firewall. Riverbed Modeler Academic Edition is used as a tool to perform simulation and analysis data. In this paper also discuss about parallel firewall in order to limit the network delay.

ABSTRAK

Pada masa kini, konsep pengasingan LAN bagi rangkaian institusi tidak lagi boleh diguna pakai. Perkara ini sama juga dengan Kolej Cosmopoint Melaka. Internet memainkan peranan yang penting dalam institusi ini. Jadi, firewall menjadi merupakan komponen penting dalam meningkatkan keselamatan rangkaian. Ia boleh memeriksa semua trafik yang keluar dan masuk ke dalam rangkaian. Kertas kerja ini memberi gambaran keseluruhan tentang firewall, kepentingannya, jenis firewall dan mengkaji kesan melaksanakan firewall kepada prestasi rangkaian. Riverbed Modeler Academic Edition digunakan sebagai alat untuk melakukan simulasi dan analisis data. Dalam kertas kerja ini juga membincangkan tentang firewall selari dalam usaha untuk menghadkan kelewatan rangkaian.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere acknowledgement to my supervisor PM Dr Abdul Samad Shibghatullah for his essential supervision, support and encouragement towards the completion of this dissertation.

I would also like to express my greatest gratitude to examiner lecturers, PM Dr. Mohd Faizal bin Abdollah and Dr. Asmala bin Ahmad for advice and suggestions in improve my dissertation report.

Special thanks to my beloved mother, father, siblings, fiancé and all my colleagues, for their moral support in completing this master project.

Lastly, thank you to everyone who had been associated to the crucial parts of realization of this master project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1   Overview

Cosmopoint College (CC) Melaka located strategically in the middle of Melaka town begin as Cosmopoint International College of Technology (CICT). It was established in year 1992. Cosmopoint College Melaka is one of the private higher education institutions under Cosmopoint Group of Companies. Cosmopoint College has 11 campuses around Malaysia including East Malaysia. Growing over 300 students in a campus college may have contributed to the increase of network traffic and network security.

Nowadays, the concept of having isolated Local Area Network (LAN) for any institution network is no longer relevant. This thing same goes with the Cosmopoint College Melaka institution with 24-hour Internet access. Internet became is an essential part and plays an important role in this institution. Everyone needs to be online and have Internet access to do lots of things. There are several advantages of having Internet in institution such as can communicate with others via email and WhatsApp messenger, a source of abundant information and resources, easy sharing of information and doings some marketing promotion via social media like Facebook and more.

While the introduction of the Internet can contributes too many benefits for the users, but just in mind, it also came with the drawbacks. Most significantly, Internet can exposed institution network to various kinds of internet threats. The most recent security threats are phishing, spyware, adware, viruses, worm, Trojan horses and etc. All of these threats are

1

potentially to access the computer system and damage it. Indirectly, this situation will gives negative impact at Cosmopoint College Melaka security and user privacy.

Based on this situation, Cosmopoint College Melaka would prioritize safety of their networked resources, availability of its network, confidentiality and integrity of its stored or transmit information. Availability ensure the data, resources or computer system is always available and accessible for authorized use whenever needed especially during emergencies situation. Whereas confidential means unauthorized user or process cannot access to the information or computer system without permission. Lastly, integrity can be define as to keep the data and information from intentional or accidental changes. (Merkow and Breithaupt, 2014).

In current situation, based on total number of user in Cosmopoint College Melaka, is not really practical to protect workstation individually. The opinion to use a firewall as a single block point to isolate the local network from the public network is a good approach to secure the network. Firewall is an important components in improving network security that prevents a network from unauthorized access. It's will filter all the in and out traffic of the network.

A firewall is a hardware or software based component that controls and monitor all the traffic across the network based on firewall rules. It also can be implemented in both software and hardware. The basic function of the firewall is to inspect or examine each packet in the network. All the packet will traverse via firewall before leaving or entering the network. For those packet that do not meet firewall security rules criteria in database will be dropped and do not allow to enter the network.
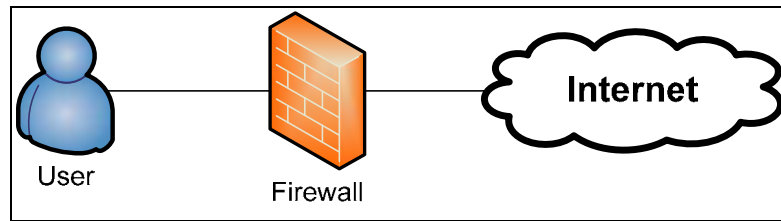
Figure 1.1: Firewall Architecture

There are three basic types of firewalls. These are packet firewall, state-full firewall and proxy firewall. Packet firewall is one of the most basic firewalls, functioned as packet filters in a network. It inspecting the packets that are transferred between computers on the Internet against the firewall's rule set. Any packets that are not meet the specifically firewall rules will dropped before reach to the receiver. That means that packet will not forward to their destination.

A second type of firewall is state-full firewall. A state-full firewall improves on the function packet filters by keep track on the state of the network connections such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) communication. Besides make a filter based on administrator defined rules, it also monitors all connections passing through it and record the data in dynamic state tables. Then, this data is evaluated properly and use that information for filtering decision. Filtering decision would be based on the history of network connection whether a packet is initiated from new connection, a part of an existing connection, or not part of any connection. If a packet does not meet any existing connection information, then its will filter based on the rule setting for new connections. It is the most efficient and cost effective firewalls types.

The last common firewall types, is a proxy firewall which that operates at the firewall's application layer. It's much more expensive firewall, most secure type of firewall compare to the others types of firewall. It's normally used to protect data centers or high

3

value server that containing publicly access. The proxy firewalls have ability to full examine the actual content of the traffic, rather than just the network address and port number.

Although proxy firewalls can improve network security layer protection compared to packet filtering and state-full inspection, it still has limitation. Some of the issues regarding proxy firewall are limited in supporting network protocol and application. This means a new proxy agent is required for each new application or protocols that need to transit across the firewall. In addition, the installation and configuration of proxy firewalls can be more difficult than other firewall technologies. Another drawback of using a proxy firewall is a reduction of network performance. This because of the full packet inspection process perform by packet filtering firewall. It will generates much more time to inspect and interpret each incoming and outgoing packet.

According to British Cambridge Dictionaries Online, performance means how well a person, machine, devices or etc. does a piece of work or an activity. Meanwhile, in Technopedia Dictionary, network performance is defined as the analysis and review of collective network statistics, to define the quality of services offered by the computer in a network. This primarily measured by quality of services delivered to the user. Broadly, network performance metric can be measured based on several network components as the following below.

- Network bandwidth or capacity

- Network throughput

- Network delay, latency and jittering

- Data loss and network error

In computer networking field, network bandwidth or capacity commonly refers to the maximum available data that can be transferred in a specific time across the network. It

4

represents the amount of data transfer capacity that can be support of a network connection in theoretically (Mitchell, 2016). Network bandwidth is usually measured in bit per second (bps). For example, IEEE 802.11g standard which is refer to the wireless technology bring 54 Mbps data rate and IEEE 802.3, Ethernet technology standard support 10 Mbps, 100 Mbps and 1000 Mbps starting with the traditional Ethernet, follow by Fast Ethernet and Gigabit Ethernet technology. Bandwidth requirement for each application are differ based on the types of application. For example, video based application require more bandwidth compare than audio and data based application.

Meanwhile, network throughput referring to the amount of data successfully transferred over the network in a given period of time. In other word, throughput means the actual capacity that data can be transferred in a network. The difference between throughput and bandwidth is bandwidth refer to the amount of data transfer in theoretical concept meanwhile throughput refer to the total amount of data transfer rate in real environment. For example, if bandwidth offer for wireless technology is 54 Mbps, the user will not exactly get full access to the 54 Mbps. This means the total amount of throughput that will be access by user is less than 54 Mbps.

Next discussion issues are network delay, latency and jittering that will affecting the speed of a network. This refers to any network issues causing packet transfer to be slower than as usual. A good network design will make a user experience a minimize delay time. For example, on the cable internet connection technology, acceptance latencies is less than 100 milliseconds (ms). Latency can be measure by Internet Control Message Protocol (ICMP) test like ping and trace route. This network tools can determine the time packet takes to travel form source to the destination. Ping test usually use to check the availability

5

connectivity of the host in the network meanwhile traceroute command is used to trace the route path that packet takes to travel in the network.

Lastly is a data loss and network error. Data loss or network error reflect to the number of packet dropped or lost in transmission and delivery process. Network errors occurs when TCP connection is timeout or the server is closing the connection. Data loss usually related with the others component such as the total amount of bandwidth and delay in a network. For example, the data loss will happen because of the dropped packet. In a network, there are buffer to queue packet at receiver places. If the queues in the network already full and not enough space to place the arriving packet the dropped packet will happened. It's called network error or data loss.

In Cosmopoint College Melaka, the network performance became a crucial issues because encounter slow network performance can leads to the staff and student frustration and stress. In addition, this is education institution where Internet play important role to search information. Besides that, all staff need to access a system that require good Internet connection access. However, before improving the network speed, one needs to know what is causing the network slow. So, this the one factor to study about relationship between firewall and network performance.

1.2   Problem statement

A firewall is an organization's first line of defense against network threat. It used to secure private network by filter incoming and outgoing packet whether to accept or reject the packet. To prevent network threat, firewalls must inspect each packet that enter or leave the network, allowing permitted traffic while discarding all other deny connection request. This activity will contribute to increase processing time for reading and interpreting packet.

6

In general, this can have a minor impact on network speeds or create reduction of performance.

So, this is one of the reasons to study the effect of implementing a firewall on to network performance. Then, a strategy to overcome the network performance issues regarding firewall deployment is proposed. In this project, the proposed solution to overcome this network performance issues by implement parallel firewall.

1.3   Research question

The main question for this research project is "How to improve network performance while implement firewall in the network". Related to the main question, a few question need to answer first.

- How firewall is function?

- How firewall will affect the network performance?

- How to improve network performance by using firewall?

1.4   Research objectives

Research objective refer to the aims to be achieve in this research project. This research project embarks on the following objectives

- To studied the effect of implementing a firewall on network performance at Cosmopoint College Melaka.

- To implement parallel firewall for improve the network performance.

- To analyse and evaluate the network performance in term of response time and delay.

1.5　Research Scope

This study will conducted at Cosmopoint College Melaka in limited time. The reason why choose the Cosmopoint College Melaka because of it is a small organization that need cost effective firewall implementation. This give an opportunity to study about Cosmopoint College Melaka network performance and improve its network. The secondary data will be used in this research project. The data will collected from internal organization with the permission of the organization using firewall log and speedtest.net application.

In this project, the testing are not implement in a real environment. It will executed in experimental or simulated environments due to the high cost and risk it takes. Riverbed Modeler Academic Edition 17.5 software will be used as a tools for this project. The reason for chosen Riverbed Modeler in this study because of the variety of features that it offers. Riverbed Modeler offers a user friendly Graphical User Interface (GUI) for the topology design. It's allows for realistic simulation of networks, has a performance data collection and variety of display module. Besides that, Riverbed Modeler provides realistic analysis of performance measures parameter.

The simulator is running on a Lenovo Idea pad 305 notebook, Intel Core i5 processor, 2.20 GHz processor speed, 1Terabytes of hard disk, 4.0 GB RAM (Random Access Memory) and Windows 10 (64 bit) operating system. The data that will be capture in this project are packet size and delay.

1.6　Research Method

Experimental research will be used as the main method in this project. Experimental research according to (Oskar Blakstad, 2008) is commonly used in sciences such as

8

sociology and psychology, physics, chemistry, biology and medicine etc. The details of this method stated in Chapter 3.

1.7 Significant Of the Study

The purposed of this project is to study the effect of implementing a firewall on network performance and to find a solution that can overcome this problem. The contributions of this project are as follows:

- Provide overview reported the experimental results of simulation.

- Propose strategies that can be used by IT Executive to maintain network performance while implement firewall.

- This research proposed a cost effective strategy to implement at all small organization.

1.8 Expected Outcome

The expected outcome of this project, Cosmopoint College Melaka was a good performance and services in Internet connection. It easier for all student and staff to get information, access to the system and server without delay. Hopefully, with implement parallel firewall at Cosmopoint College Melaka the network becomes stable and don't have any Internet interruption. It will convenience to all the user want to access the Internet.

9

1.9 Summary

Table 1.1: Summary of the Project

Research Problem	Research Question	Research Objectives	Research Method	Research Contribution
Network performance at Cosmopoint College Melaka has problem such as has frequent outages and the network becomes extremely slow when all user want	How firewall will affect the network performance?	The first objective is to study the effect of implementing a firewall on network performance at Cosmopoint College Melaka.	Form hypothesis.	Significant to IT Executive to maintain the network performance and provide robust, reliable and availability Internet services to the user at CC Melaka.
	How to improve network performance by using firewall?	The second objective is to propose a solution which is implement parallel firewall for improve the network performance.	Perform experiment, testing and analysis the response time and delay using Riverbed Modeler.	