PERFORMANCE COMPARISON ENCRYPTION

OF IPSEC VPN ENCRYPTION TECHNIQUES

NUR HASYIMAH BINTI MOHD RIDZUAN

FACULTY OF ELECTRICAL ENGINEERING

UNIVERSITI TEKNOLOGI MARA

MALAYSIA

ACKNOWLEDGEMENT

Praises to Allah for His Blessings and the knowledge He bestowed upon us. With His help and guidance, I am able to accomplish this project successfully. Here, I would like to express my sincere gratitude and appreciation to my supportive supervisor, Assoc. Professor Ruhani Ab Rahman, who is always give support and guidance all through this Project. To my colleagues, all part time student batch 2012 thanks for their cooperation and supportive ideas. Other than that, highly appreciate to my family and husband Abdul Rashid Hussain for their continuous support and encouragement. I owe my gratitude to all those people who have made this project possible especially Suraya and Nur Hayati.

ABSTRACT

Internet Protocol Security (IPSEC) is one of the protocol implements in VPN site to site tunnels network. Where Virtual Private network (VPN) is a technology that used to transmit information via insecure regions such as internet from one office on one geographical area to another geographical area. IPSEC protocol network setup encrypt the overall IP traffic packets before being transferred from source to destination in order to secure the tunnels. This paper presents the implementation of site to site VPN tunneling using a network simulator. By varying the combination of encryption algorithm 3DES and AES 256 with two hashing type SHA-1 and MD5, the performance of each algorithm was compared and analyzed via Window 7 environment. The implementation of IPSEC protocol via Cisco equipments was introduced. Results indicate different algorithms (with and without encryption), hashing method and packet length have influence on Round Trip Time (RTT) result.

CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Background of Study

Nowadays the expanded of Internet functionality was rapidly used as a default communication platform for all area of life including in business, study, politics, hospitalization and many more. The continuous growth of Internet Protocol (IP) functionality has leaded the user to widely use the technology in various platforms such as via mobile devices and computer communication. The main purpose is to allow the data transmission, changing information and sharing resources across the network. However, the TCP/IP protocol on internet environment was not setup with data security features during the transmission of packet transfer. Meaning that, for any transmission of information across the network for communication reason, no assurance and authorization access upon data content since the data transmit and receives is consider as vulnerable sources. As an alternative solution, many researchers have come out with several solutions to abolish the limitation and problematic security issue. By that, Virtual Private Network (VPN) tunnelling was developed and introduced to eliminate and overcome the negative effect on user side. Today, it becomes most common methods apply and consider as a trusted technology to ensure the data transmission via unknown network resources can be completely secure. For example, the new services such as teleconference, e-commerce and e-banking can widely used after the implementation of VPN tunnelling since it allows well designed of data security protection, authentication and data confidentiality. Moreover, instead of using conventional method of leased line and dialled up network, the benefits of VPN tunnelling functionality can be highlighted such as able to reduce the overall communication costs to the related industry, permits the vendor or business partner to communicate via secure network remotely, offer high level of security data transmission and the network architecture itself able to produce convenience in terms of dynamic structure and maintenance support.