UNIVERSITI TEKNOLOGI MARA

PERFORMANCE COMPARISON ANALYSIS OF AES-256 SHA-256-HMAC, AES-256 MD5-HMAC, 3DES SHA-256-HMAC AND 3DES-MD5-HMAC ON IPSEC VPN USING GNS3

MOHD HILMAN BIN LUKMAN

Dissertation submitted in partial fulfillment of the requirements
for the degree of

Master of Science

Faculty of Electrical Engineering

January 2016

ABSTRACT

Encryption algorithm will take advantage of advance computer hardware in term of processing and memory capacity. Secure connection can be established between two points within public internet infrastucture. To not compromise the resources of end terminal, this encryption and decryption process is done at layer 3 network. However performance of encryption needs to be tested as so many encryption algorithms in the market.

This paper presented performance comparison analysis between two encryption algorithms and two integrity algorithms. The performances of the algorithm are compared by monitoring the download speed or throughput of every algorithm. By varying the algorithm, file size and protocol, every throughput is compared. Combination algorithm AES-256 SHA-256-HMAC has the highest throughput among others. The analysis also found that FTP performs better than HTTP. All the experiments are using GNS3.

ACKNOWLEDGEMENT

First and foremost, praise to Allah S.W.T for His willing and blessing in giving me the opportunity and strength to complete my Master's degree generally and my final year project specifically. I would like to express my gratitude to my supervisor Dr Yusnani Yusoff for inspiration and guidance throughout the process of completing this thesis.

I also want to thank my wife Pn. Syarina binti Mohd Hairon and my kids for understanding and giving me time and space to finish this project.

Finally, I would like to thank my friends and all EE700 students who help me and gave me unwavering support.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 RESEARCH BACKGROUND

About 20 years ago internet become very popular when personal computer was introduced. After that, the usages of internet are increasing when laptop becomes affordable, and lately when Smartphone become very popular the usages of internet are booming. In line with increasing of internet usage there are demands for security and reliable data transfer or communication through the internet.

The easiest way to get the secure communication through the internet is via VPN. VPN can be implemented in the public internet network, and because of that VPN are low cost, high scalability and reliable compared to the least line.

There are four common protocols used for creating VPNs over the Internet:

- Point-to-point Tunneling Protocol (PPTP)[1]
- Layer 2 VPN[2][3]
- Secure Socket Tunneling Protocol (SSTP)[4]
- IP Security Protocol (IPSec) [5][6]

Among these, IP security protocol is the most popular. IP security protocol that use together with TCP/IP protocol are very versatile. Since IP security protocol is implemented at layer 3, performance of the terminal equipment and layer 2 networks is not affected.