

**Universiti Teknologi MARA**

**Netguard: Implementing OpenVPN, Pi-Hole and IDS for Securing Network Environment Using Raspberry Pi Technology**

**Muhammad Tholhah Bin Zabri**

**Thesis submitted in fulfilment of the requirements  
for Bachelor of Computer Science (Hons.) Data  
Communication and Networking  
Faculty of Computer and Mathematical Sciences**

**DECEMBER 2018**

## **STUDENT DECLARATION**

I certify that this report and the research to which it refers are the product of my own work and that any ideas or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline.

.....

MUHAMMAD THOLHAH BIN ZABRI

2016340751

DEC 10, 2018

## ABSTRACT

Living in this modern world with almost every electronic device are connected to the internet where everything is at the tip of a finger, but do they know that they are being monitored. Only a few people take notice of their sensitive data being monitored by Internet Service Providers (ISPs) and other third-party company. Besides, every site they visit, every input they fill in search box or form and every click on the website are being tracked by a third-party company that wanted to know the user's interest and then will pop up advertisement which related to the user's interest. This will become a problem when the third party have all the sensitive information and will misuse it in the wrong way. That is why a device or tool is needed to protect the user from falling into the internet "pitfall". A device with a capability to hide user's Internet Protocol (IP) and at the same time to protect the user from any tracker and advertisement from the internet is developed in this project. The idea of this project is to hide the user IP by masking it with OpenVPN server that is deployed in another country then making it safe for the user from being tracked by an attacker from the internet. Then, to block any Domain Name System (DNS) request for known tracking and advertising domain by using Pi-Hole project that is being maintained by the online community. After that, to provide additional protection, Raspberry Pi with the help of Suricata IDS is used in the network to act as the default gateway for the user and to prevent the Man-in-the-Middle attack from inside the network. The difference in network performance between before and after applying NetGuard does not vary too much and it also does not drop the network connectivity and performance which may cause disturbance to the user.

# TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
<b>SUPERVISOR’S APPROVAL</b>	<b>i</b>
<b>STUDENT DECLARATION</b>	<b>ii</b>
<b>ACKNOWLEDGEMENT</b>	<b>iii</b>
<b>ABSTRACT</b>	<b>iv</b>
<b>LIST OF FIGURES</b>	<b>viii</b>
<b>LIST OF TABLES</b>	<b>x</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xi</b>
<b>CHAPTER ONE: INTRODUCTION</b>	<b>1</b>
1.1    Background of Study	1
1.2    Research Motivation	2
1.3    Problem Statement	3
1.4    Research Objective	5
1.5    Research Scope	5
1.6    Research Significance	5
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>6</b>
2.1    Virtual Private Network (VPN)	6
2.1.1    OpenVPN	8
2.1.1    Tor Network	9
2.2    Advertisement	12
2.2.1    Advertisement Blocker	13
2.2.2    Pi-Hole	14
2.3    Intrusion Detection System (IDS)	15

<b>CHAPTER FIVE: TESTING AND ANALYSIS</b>	<b>51</b>
5.1 NetGuard Capability Testing and Analysis	51
5.1.1 OpenVPN Anonymity and Leak Testing	52
5.1.2 Advertisement and Tracker Blocking Testing with Pi-Hole	57
5.1.3 IDS Testing with Suricata	62
5.3 Summary	67
<b>CHAPTER SIX: CONCLUSION AND RECOMMENDATION</b>	<b>68</b>
6.1 CONTRIBUTION	68
6.2 PROJECT LIMITATION	69
6.3 RECOMMENDATION AND FUTURE WORKS	70
<b>REFERENCES</b>	<b>72</b>
<b>APPENDICES</b>	<b>75</b>
APPENDIX A - Pairing Pi-Hole with OpenVPN	76
Installation of OpenVPN	76
Installation of Pi-Hole	76
Integrate Pi-Hole with OpenVPN	78
APPENDIX B – Raspberry Pi Setup	80
OpenVPN Client Setup	80
Enable IP Forwarding	80
APPENDIX C – Installing Suricata IDS	82
APPENDIX D – Suricata IDS Web GUI	83