Implementing Stackable Open-Source Firewall Security and Network Traffic Monitoring System

Ariyarathne K.A.S.
MS20902902

M.Sc. in IT
Specialized in Cyber Security

Supervisor: Dr. Lakmal Rupasinghe

January 2020

Department of Computer Science
Faculty of Graduate Study and Research
Sri Lanka Institute of Information Technology

Table of Contents

Table of Contents 2

List of Figures 4

List of Tables 5

Abstract **6**

Chapter 1 Introduction and Project Details 7

1.1 Background **7**

1.2 What is Firewall? **7**

1.2.1 Proxy firewall 8

1.2.2 Stateful Inspection Firewall 8

1.2.3 Unified Threat Management firewall (UTMFW) 8

1.2.4 Next Generation Firewall (NGFW) 8

1.2.5 Threat focus-next generation firewall (Threat Focus-NGFW) 9

1.2.6 Virtual firewall 9

1.3 What is Network Monitoring? **9**

1.3.1 Fixed Network Traffic Monitoring 10

1.3.2 Random Network Traffic Monitoring 10

1.3.3 Router-based Network Traffic monitoring 10

1.3.4 Simple Network Monitoring Protocol (SNMP) 11

1.3.5 Remote Monitoring (RMON) RFC 1757 11

1.3.6 NetFlow RFC 3954 11

1.4 Significant of the study **11**

1.5 Problem Definition **12**

1.6 Objective of the research **12**

1.6.1 General Objective 12

1.6.2 Specific Objective 12

Chapter 2 Background and Literature Elaboration 13

2.1 Literature review **13**

The Open-Source Firewall 13

2.1.1 OPNSense Firewall 14

2.1.2 PfSense Firewall 14

2.1.3 IPFire Firewall 14

2.1.4 NG Firewall 14

Open-Source Network Monitoring 15

2.1.5 Open-source platform-ELK Stack 15

2.1.6 Elastic Search 15

2.1.7 Logstash 16

2.1.8 Kibana........ 24

2.1.9 Why ELK Stack? 25

Chapter 3 Development........ 25

3.1 Methodology 25

3.1.1 Theoretical framework........ 25

3.1.2 Installing OPNSence 27

3.1.3 Installing Elastic Search on Windows 10 VM 30

3.1.4 Installing Kibana on Windows 10 VM 32

3.1.5 Installing Logstash on Windows 10 VM 35

3.2 Requirement Analysis and Gathering........ 36

3.2.1 Software Requirements 36

3.2.2 Hardware Requirements........ 36

3.3 Design 37

3.3.1 Event List ....**Error! Bookmark not defined.**

3.3.2 Flow Chart Diagram........ 37

3.3.3 Site Map 38

Chapter 4 Testing cases and Result Analysis 39

Chapter 5 Conclusion and Future Works 39

Chapter 6 Social, Ethical and Legal Issues of the project........ 39

Bibliography 39

Appendix 44

Appendix 1: Gantt Chart 44

Appendix 2: Work Breakdown Structure .... Error! Bookmark not defined.

List of Figures

Figure 1: ELK Stack three stages 15
Figure 2: Kibana Dashboard 24
Figure 3: Creating New Virtual machine 27
Figure 4: Attaching two NIC 27
Figure 5: Connecting first NIC to LAN & second NIC to NAT 28
Figure 6: Installing OPNSense Firewall 28
Figure 7: Configure Firewall interface cards 29
Figure 8: OPNSense Firewall Web interface. 29
Figure 9: ElK Stack official web site 30
Figure 10: Elastic Search, Logstash, and Kibana Zipped and unzipped file in C directory 30
Figure 11: Elastic Search bin folder file path 31
Figure 12: Access the Elastic Search bin folder path with CMD 31
Figure 13: Running Elastic Search batch file via CMD 31
Figure 14: Elastic Search login with localhost: 9200 32
Figure 15: Kibana bin folder file path 32
Figure 16: Access the Kibana bin folder path with CMD 33
Figure 17: Running Kibana batch file via CMD 33
Figure 18: Kibana running states 34
Figure 19: Kibana first dashboard 34
Figure 20: Adding ELK variables to the system 35
Figure 21: Creating logstash.conf file 35
Figure 22: Running Logstash via CMD 36
Figure 23: Flow Chart Diagram 37
Figure 24: Site Map Overview of the system 38

List of Tables

Table 1: Firewall Comparison.. 13

Abstract

Network security is the main feature in network management. For that firewall and network monitoring systems are the main ingredients. Around the world millions of dollars annually are spent by the organizations for safeguards their data and information from unauthorized accesses. In the current market there are two type firewall and monitoring tools available for users, commercial and open source. But all these tools are not suitable for entry level, small and medium sized enterprises (SME's). The commercial Firewalls and Network monitoring tools are dead weight for entry level and small size businesses, both financially and functionally. For that most efficient and available solution for that is to move to open-source firewall and network traffic monitoring systems. But the firewall should be armed with next generation firewall features such as UTM filtering, URL filtering, antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering, leak prevention, remote routing, NAT, and VPN support. And Network traffic monitoring should be included with network devices, links and connections, mission critical servers, external service providers, passive/active network health monitoring, automatic alerts, automatic load balancing and failover, monitor abnormal behaviors, etc. And finally, as a tool kit open-source firewall and network traffic monitoring systems work as a single unit to prevent, detect, and disable network attacks.

Key words: firewall, network security, network traffic, network monitoring