



**“FireX” – A Low Cost Raspberry Pi
Based Open-Source Firewall Appliance
for Sri Lanka Post**

G.G.U Fernando
(Reg. No.: MS20909864)
M.Sc. in IT
Specialized in Cyber Security

Supervisor: Dr. Lakmal Rupasingha

December 2021

Faculty of Computing
Sri Lanka Institute of Information Technology

Abstract

“FireX” – A Low Cost Raspberry Pi Based Open-Source Firewall Appliance for Sri Lanka Post

G.G.U Fernando

MSc. in Information Technology (Cyber Security)

Supervisor: Dr. Lakmal Rupasinghe

December 2021

Recent statistics on data breach shows millions of data get stolen or lost every year and larger organizations are moving in to complex IT security solutions to protect their data from the intruders. However, organizations with limited financial capabilities remain unprotected to lack of available funds to invest on decent IT security solution for their organization. Department of Posts Sri Lanka (Sri Lanka POST) is also in a situation where seeking a low cost IT security firewall solution to protect their post offices located around the country. The open source firewall solutions are the most popular world-wide methodology for used to empower the overall security of a medium scale home and office computing network as well as large scale cooperate networks without spending a large amount of funds. Open Source Firewall Controls embedded to a hardware device provides more centralized approach for IT Engineers when managing a network. Furthermore, most of other Government Organizations in Sri Lanka faces the same issues when protecting their cooperate network infrastructure due to financial capabilities. As a solution, The Researcher designed an open source low cost embedded hardware device to act as a corporate firewall where the device can govern the network access while catering the business requirements whereas protecting the IT assets from the intruders. The designed firewall solution is based on multiple open source packages which can run on a raspberry pi model 3b+ single-board computer (SBC). The open source firewall package ‘IPFire’ was used to act as the firewalling module for this project. At the end of this research project the Researcher is planning to locate on post offices around Sri Lanka.

Acknowledgements

I would like to thank Dr. Lakmal Rupasinghe for his encouragement, support and insightful comments provided make this research a success. Also I am truly grateful to my family for their encouragement, motivation and love. Without them this work would never have come into existence.

I would like to thank the Postmaster General and Deputy postmaster general to allow me to use Department of posts information in my research. Also I would like to thank mr.Priyankara perera from Sri Lanka Cyber Security Readiness Team to support me to find some resources.

.

Table of Contents

List of Figures	vii
List of Tables	ix
Chapter 1	1
Introduction	1
1.1 Background	1
1.2 Concept & Area of Study	2
1.3 Dissertation Structure	2
1.4 Research Objectives	3
Chapter 2	4
Literature Review	4
2.1 Previous Efforts	4
Chapter 3	6
Architecture & Preparation	6
3.1 Introduction - Raspberry Pi Single Board Computer	6
3.1.1 Raspberry Pi SBC Hardware Layout	6
3.2 Introduction – IPFire Open Source Firewall Package	7
3.2.1 IP Fire Architecture Layout - Network	8
3.2.2 IP Fire Architecture Layout – Software	8
3.3 High Level Design Diagram – Hardware	9
3.4 High Level Design Diagram – Software	10
Chapter 4	11
Methodology	11
4.1 System Preparation	11
4.1.1 Preparation of Software Modules	11
4.1.1.1 Acquisition of IPFire ARM Image	11
4.1.1.2 Acquisition of balenaEtcher	11
4.1.1.3 Flashing IPFire ISO image	12
4.1.1.4 Configuring Serial Console on Raspberry Pi SBC	13
4.1.1.5 First-time boot up IPFire on Raspberry Pi SBC	13
4.1.2 Preparation of Hardware Modules	17
4.1.2.1 Hardware Arrangement	17
4.1.2.2 Mounting IPFire Micro SD Card	18

4.1.2.3 First Time Boot - From the SD Card	18
4.2 Configuring IP Fire Package	19
4.2.1 Setting Up Network Interfaces	20
4.2.2 Setting Up Firewall Rules	21
4.2.3 Setting Up Routing Table	21
4.2.4 Setting Up DNS	22
4.2.5 Setting Up Web Proxy	22
4.2.6 Setting Captive Portal	23
Chapter 5	24
Results	24
5.1 Physical Hardware Firewall	24
5.2 Implementation of Firewall Features	25
5.2.2 Routing Table	26
5.2.3 DNS Settings	26
5.2.4 Proxy Server	27
5.3 Implementation of Captive Portal	27
5.4 Implementation of Wireless Network	29
5.5 Testing Environment	30
5.5.1 ARM Installation	31
5.5.2 Test Results & Statistics	31
5.5.3 Final Hardware Layout	34
Chapter 6	37
Discussion	37
6.1 Limitations and Opportunity for Improvements	37
6.1.1 Implementation of Intrusion Prevention Module	37
6.1.2 Open VPN Module	38
6.1.3 Hardware Switch for Shutdown	39
Chapter 7	i
Conclusion	i
8.1 The Way Forward	i
References	ii

List of Figures

Figure 2.1 IPFire Implementation by Tom's Hardware	4
Figure 2.2 Oğuzhan Karahan and Berat Kaya's Approach	5
Figure 2.3 Wojciech Quibell's Approach.....	5
Figure 3.1 Evolvement of the Raspberry Pi SBC	6
Figure 3.2 Hardware Layout of the Model 3b+	7
Figure 3.3 High Level Fire Architecture Layout of IPFire.....	8
Figure 3.4 Logo - Project Pi-hole	9
Figure 3.5 Logo - Project Squid	9
Figure 3.6 High Level Design Diagram – Hardware.....	10
Figure 3.7 High Level Design Diagram – Software	10
Figure 4.1 IPFire ARM Image ISO	11
Figure 4.2 'balenaEtcher' software	12
Figure 4.3 Flashing IPFire ISO image.....	12
Figure 4.4 Integrity Validation	12
Figure 4.5 Configuring Serial Console.....	13
Figure 4.6 IP Fire Installation Console.....	13
Figure 4.7 Setting Hostname	14
Figure 4.8 Configuring Network Layout.....	14
Figure 4.9 Network Adapter Layout	15
Figure 4.10 Network Adapter Assignment.....	15
Figure 4.11 DHCP Lease Assignment.....	16
Figure 4.12 DHCP Lease Assignment.....	16
Figure 4.13 Web Based GUI	17
Figure 4.14 Hardware Arrangement	18
Figure 4.15 Mounting IP Fire SD Card	18
Figure 4.16 First Time Boot Process	19
Figure 4.17 IP Fire Web UI.....	20
Figure 4.18 Setting Network Interfaces.....	20
Figure 4.19 Setting up Firewall Rules	21
Figure 4.20 Setting up Routing	21
Figure 4.21 Setting up DNS	22
Figure 4.22 Setting up Web Proxy	22
Figure 4.23 Setting up Captive Portal	23
Figure 5.1 Hardware Firewall	24
Figure 5.2 Available Ports.....	25
Figure 5.3 Firewall Rules HTTP and HTTPS Traffic	25
Figure 5.4 Running Routing Table Configuration.....	26

Figure 5.5 DNS Resolvers	26
Figure 5.6 Proxy Server Configuration	27
Figure 5.7 Captive Portal Settings.....	28
Figure 5.8 Captive Portal Welcome Screen.....	28
Figure 5.9 Captive Portal Session Expiry.....	28
Figure 5.10 Hardware arrangement for the wireless interface.....	29
Figure 5.11 DD-WRT based firmware	29
Figure 5.12 Wireless Network.....	30
Figure 5.13 Test Environment.....	30
Figure 5.14 'armv5tel' support	31
Figure 5.15 DHCP Allocation	31
Figure 5.16 DHCP Lease Table.....	31
Figure 5.17 Peer Connections	32
Figure 5.18 Data wise utilization of the LAN (Green) interface	32
Figure 5.19 Load Average - 5 Minute	33
Figure 5.20 Load Average - Hourly, Daily and Monthly	33
Figure 5.21 Final Hardware Layout	34
Figure 5.22 Final hardware layout with the system access.....	34
Figure 5.23 LAN and WAN Interfaces	35
Figure 5.24 VGA (Display) and USB Interfaces.....	35
Figure 5.25 Activity Lights	36
Figure 6.1 Intrusion Prevention System (IPS) module.....	38
Figure 6.2 Open VPN Module	39
Figure 6.3 Shut off Procedure	39

List of Tables

Table 4.1 IP Addressing schema	15
Table 6.1 Sub Objectives addressed in each chapter	37