Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 303-308

Designing a Firewall System for a Computer Network Based on a Single-Board Computer

Krasimir Slavyanov
Department Computer Systems and Technologies
"Vasil Levski" National Military University
Shumen, Bulgaria
k.o.slavyanov@gmail.com

Angela Borisova
Department Computer Systems and Technologies
"Vasil Levski" National Military University
Shumen, Bulgaria
angela.borisova@abv.bg

***Abstract* — When configuring temporary or hastily built, field or other computer networks, it is necessary that they meet all modern standards and requirements for computer networks and for cybersecurity when connecting to the Internet. This study proposes an approach for designing, configuring and setting up a firewall for a computer network, built and configured based on a Raspberry Pi single-board computer and free software. The basic configuration and operation with the various functionalities of the Intrusion Prevention System are described in detail. The application of the proposed solution is possible both for training and research in laboratory conditions and for permanent operation and monitoring of the system by specialists in real conditions and continuous operation.**

Keywords* — *firewall, intrusion prevention system, single-board computer

I. Introduction

In many cases, when it is necessary to build a computer network, this may have to be done in a short time, without the necessary funding, due to logistical or other problems, and without the full set of necessary computer and network equipment that meets all the standards for this. Often, a temporary solution to the problem can turn out to be quite long. However, it is difficult to compromise with cybersecurity, especially if we are talking about small businesses with not many users and employees and, accordingly, with small computer networks and not so serious traffic, which also have to be analyzed in some cases for special or military operations [1]. Relatively cheap solutions can offer single-board computers such as Arduino, Raspberry Pi, etc. Especially Raspberry Pi boards have proven their effectiveness, both in managing the Internet of Things (IoT) [2], Web of Things [3] - smart home systems, IoT vulnerability analysis [4], managing physical security systems, controlling robots, drones, testing cybersecurity [5], VoIP [6], wireless network [7], [8] and unfortunately, they also turn out to be some of the most dangerous devices used by malicious users of a computer network. Intrusion detection and alert supported by cloud solutions with Neural Networks is also an example of how efficient the single board computers can be [9].

This report proposes an easily feasible and sufficiently reliable solution to this problem, without investing significant financial resources, but providing basic security, firewall, gateway, router with basic capabilities. This is a computer system built based on a Raspberry Pi 4.0 single-board computer, functioning as a firewall. An open-source intrusion detection system (IDS) is designed and configured based on the IPFire firewall software.

II. Materials and Methods

The following hardware is required for the system build: Raspberry Pi 4.0 (8 GB) with power supply, USB to Ethernet adapter – supporting 1000 Mbps (USB 3.0), micro SDXC memory card (min 32 GB), HDMI to micro-HDMI adapter, HDMI cable, HDMI monitor, USB keyboard.

The software required for the installation includes the following open-source products:

- Raspberry Pi Imager (ver.2.0.7)
- IPFire 2.29 core200 (ver. aarch64, ".xz" archive)

For better understanding the research is structured in several stages, each with specific purpose.

A. Flashing the memory with the IPFire OS

To flash the proper version of the ipfire OS, it should be downloaded from the official website of the company, in our case it is https://www.ipfire.org. The version of the software needed is ver. aarch64, an archive with extension ".xz" is needed.

An important condition is that the ipfire OS should be flashed on the memory card with the Raspberry Pi official software for that purpose - Raspberry Pi Imager, which should be downloaded also from the official website of the company https://www.raspberrypi.com with version proper for the Operational System of the computer used for the purpose. The experience in that stage proved that using another software for bootable storage creation like Rufus,

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.171

Balena Etcher etc. is not a working option. Just after the flashing procedure is completed and verified it is important to change the value of the parameter SERIAL-CONSOLE to OFF, the option is in the file uEnv.txt. The content of the file should look like this:

```
KVER=6.18.7-ipfire
root_dev=UUID=10114230-2832-4935-94ac-91a6b8e43be2
SERIAL-CONSOLE=OFF
```

B. Assembling and configuring the firewall system.

For the installation and configuration of the Raspberry Pi based firewall system, the previously flashed with the ipfire OS memory card should be installed on the board. For configuration access to the board, it should have a USB keyboard attached as well as some HDMI connected display. For the monitor it is important to be attached to the first micro-HDMI port (HDMI0, the left one), otherwise a rainbow colors will be displayed.

The additional USB to Ethernet adapter – supporting 1000 Mbps must be connected to one of the pair of USB 3.0 ports, where higher data transfer rate is supported.

The need of two ethernet RJ45 ports is essential because the firewall as it is by its purpose should have one port connected to the internet provider (WAN). This stream is called RED in the IPFire software. For the needs of the approach here RED connection will be configured to use the built-in RJ45 port. The LAN connection for the firewall is called GREEN, and it is planned to be configured on the additional USB 3.0 to Ethernet adapter.

After all the assembling is done before attaching the network cable the system has to be powered on and then configured with the following network properties for the installed IPFire operational system:

1. Language and time, according to the planned system operational location.
2. Machine host name, passwords for the users “root” and “admin”.
3. Selection of the network configuration type – there are several options according to the type of the service needed:

- RED -as mentioned before is for the WAN
- GREEN – for the LAN segment
- BLUE for the local Wi-Fi network
- ORANGE – for the DMZ (web servers, financial, HR or other functional system)

For the experiment only the basic configuration type is chosen RED + GREEN, as for the firewall use between WAN and LAN.

4. Drivers and card assignments – here the selection for the RED and the GREEN network adapter should be made, a variant is shown:

```
GREEN: "usb: Realtek Semiconductor
Corp. RTL8153 Gigabit Ethernet
Adapter"
GREEN: (fc: 19:28:66:f3:3c)
RED  : "of: bcmgenet"
RED  : (d8:3a:dd:f1:0b:d1) GREEN RED
```

5. IP Address settings for the RED and GREEN interface:

- The WAN interface (RED) in the most common case uses a DHCP service, therefore the configured settings are consistent with this., shown on fig. 1.

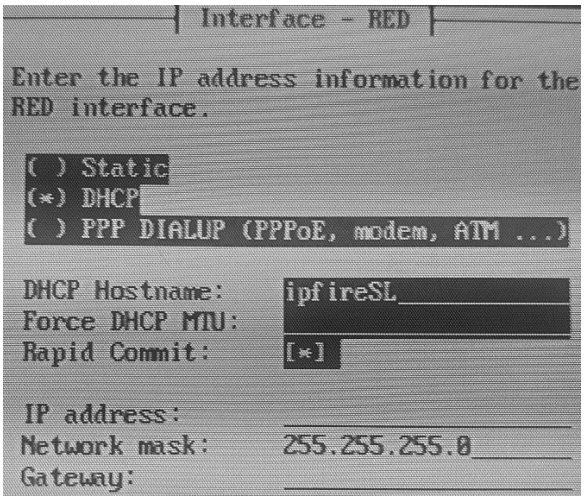

Fig. 1. Address settings for WAN (RED) interface.

- The IP address information for the LAN interface GREEN interface is configured as follows:

```
IP address:192.168.4.1
Network mask:255.255.255.0
```

The DHCP configuration is chosen to be as follows:

```
      DHCP server configuration

Configure the DHCP server by
entering the settings information.

[*] Enabled

Start address:192.168.4.58
End address:192.168.4.254
Primary DNS:192.168.4.1
Secondary DNS:4.2.2.2.
Default lease (mins): 60
Max lease (mins):120
Domain name suffix: localdomain
```

C. Firewall Software configuration.

After the installation configuration the Raspberry Pi based firewall system should be connected as described before to the WAN and LAN. It can be accessed from any computer device in the LAN. For that purpose, at first the assigned IP address has to be checked with the command “ipconfig /all” for Windows OS. The results received are:

```
Ethernet adapter Ethernet:
Connection-specific DNS Suffix:
localdomain
```

```
Description: Intel(R) Ethernet
Connection (3) 1218-LM
Physical Address: 68-F7-28-93-89-39
DHCP Enabled: Yes
Autoconfiguration Enabled: Yes
Link-local IPv6 Address:
fe80::9f9e:21e6:f1cf:2f7c%10(Preferr
ed)
IPv4 Address:192.168.4.51(Preferred)
Subnet Mask: 255.255.255.0
Lease Obtained: 26 April 2026
10:18:05
Lease Expires: 26 April 2026
11:18:05
Default Gateway: 192.168.4.1
DHCP Server: 192.168.4.1
DHCPv6 IAID: 124319528
DHCPv6 Client DUID: 00-01-00-01-2E-
F0-C1-68-68-F7-28-93-89-39
DNS Servers: 192.168.4.1
             4.2.2.2
NetBIOS over Tcpip: Enabled
```

The GUI of the Raspberry Pi device can be found typing the address 192.168.4.1:444 on any web browser software as the IPFire is using port 444.

The first step in the configuration process should be to activate the Intrusion Prevention Service (IPS) adding provider, which can be found on the Firewall menu (fig. 2).

The Snort/VRT GPLv2 Community Rules is selected as it is proven to be very effective and free. There are available some of the most popular free and not free IPS providers. The firewall has an option to visit the provider website, as well as to enable automatic updates, which in this case is chosen.

From the optional functionalities included IPsec and WireGuard as well as the RED and GREEN interface are activated. Report sending option is also available for configuration (fig. 3). After saving the selectin The IPS is automatically started.

Representing full-scale firewall functionality, the configuration of the IPFire on the Raspberry Pi 4.0 is supported Zone Configuration (fig. 4), Firewall rules (fig.5) and even Location Block services (fig.6) for blocking the traffic from one or more countries.

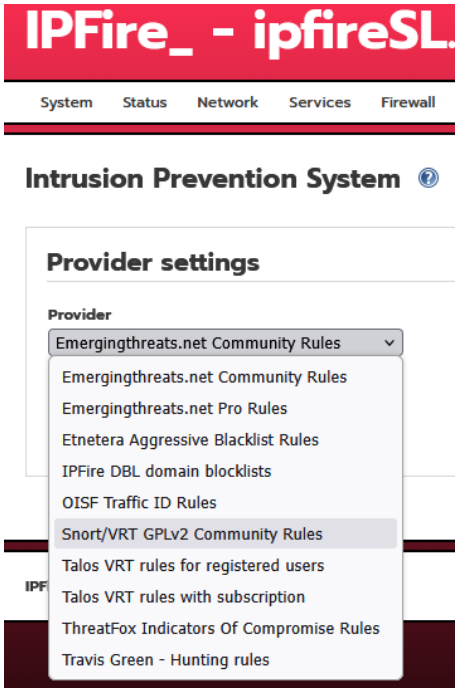

Fig. 2. Provider selection for the IPS.

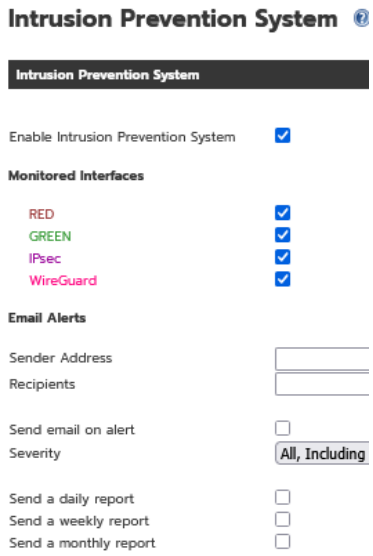

Fig. 3. Selection of the optional functionalities for the IPS.

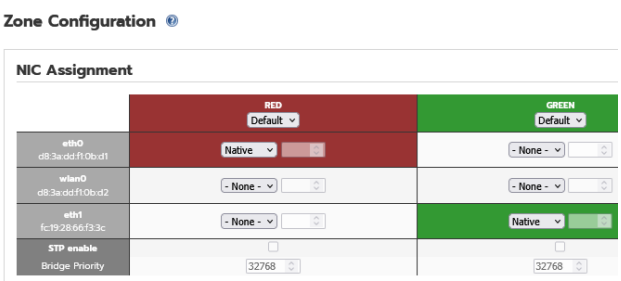

Fig. 4. Zone Configuration for the IPS.

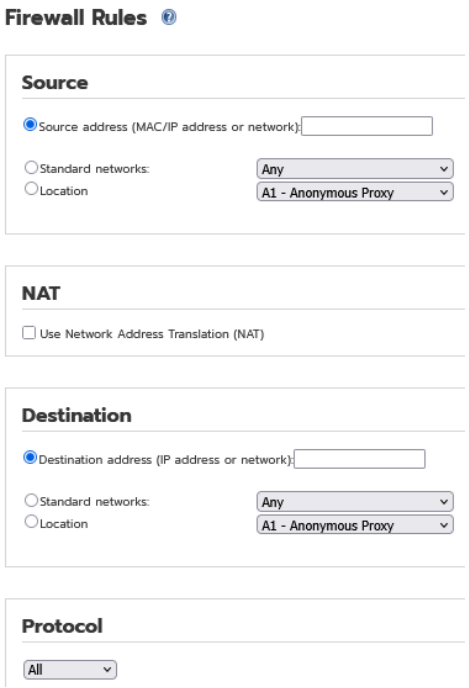

Fig. 5. Adding new rule for the IPS

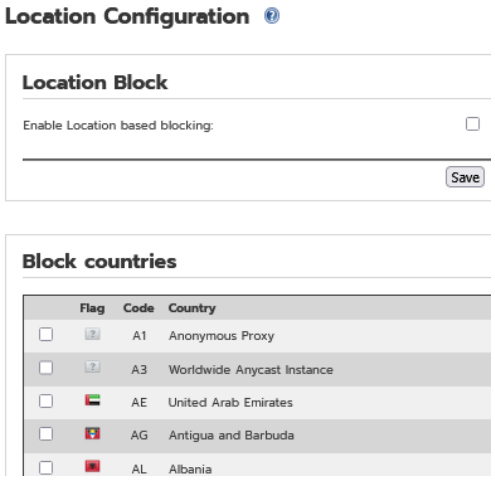

Fig. 6. Location Block Configuration.

The location log supported can be analyzed with the firewall log graph (IP) option provided. This is shown on fig. 7.

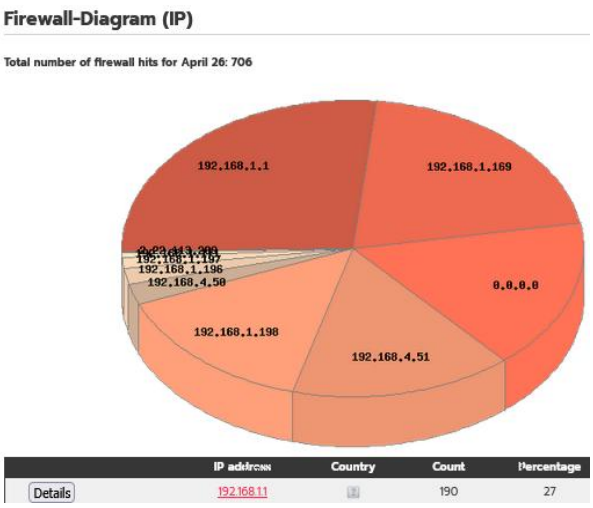

Fig. 7. Firewall log graph (IP).

The Pakfire configuration is used for the installation of some that proved to be very common firewall tools like FreeRADIUS for radius authentication (fig. 8).

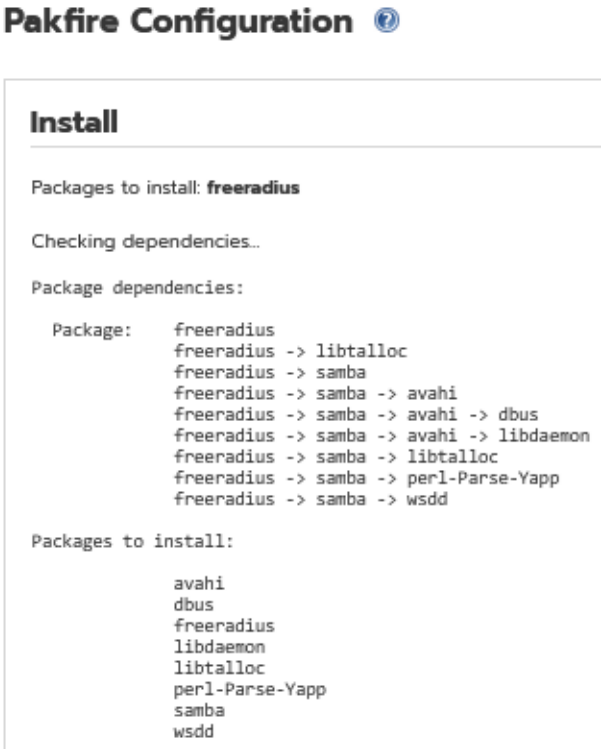

Fig. 8. FreeRADIUS installation on Pakfire Configuration.

Another available tool for capturing packets from network traffic is Tshark. One deeper analysis on the lower level is proven to be very useful if the LAN computers are targeted from outside or some unusual traffic is noticed.

III. Results and Discussion

After an hour of surfing with the firewall on, the operating temperature of the Raspberry Pi 4.0 is not at its peak. The Internet connection speed test shows that it is within the realistically expected norms ~ 85 Mbps. LAN security for a small office or home is proven to be provided

by a pocket Raspberry Pi 4.0, which can be powered by a battery for a long time due to its low power consumption.

For status information analysis, CPU performance (shown in Fig. 9) and average load (Fig. 10) can be visualized graphically on a daily, weekly, monthly, and yearly basis. The memory usage graph is visualized with maximum, average, minimum, and current captions for used, buffered, cached, and free memory displayed (fig. 11).

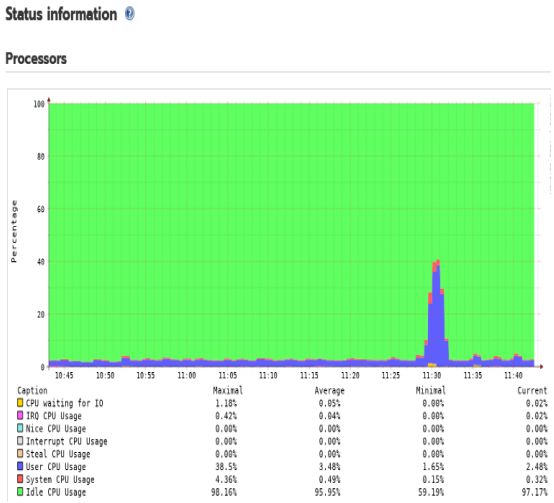

Fig. 9. Status information for the processors' work

Fig. 10. Average load status information

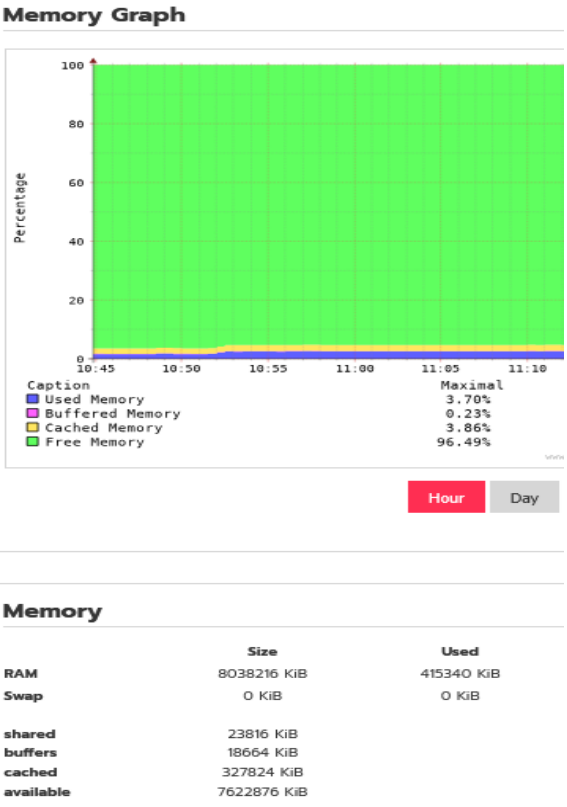

Fig. 11. Status information for the memory usage of the firewall system

IV. Conclusions

This approach offers the opportunity to build and maintain basic firewall functionality for computer systems, which can be successfully quickly installed and configured as a backup solution when the main firewall fails. Even not only as a real firewall, IPfire can be successfully used as a monitoring station to monitor for anomalies in daily business traffic. This is also one of the most successfully applied strategies of system attackers. Nowadays, detection and prevention of all types of threats from just one system is often an ability achievable with large investments.

Acknowledgments

This work was supported by the National Science Program "Security and Defence", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022. The material reflects only the author's opinion, and the Ministry of Education and Science is not responsible for the content.

References

[1] L. Nikolov, I. Zheleva, D. Mitich, "Network traffic in an intense artillery battery operation", Proceedings of International Scientific Conference "Defense Technologies", 2024, Shumen, National Military University "Vasil Levski", Faculty "Artillery, Air Defense and CIS", pp 372-378, ISSN 2815-4282

[2] C. Dow, Internet of Things Programming Projects: Build exciting IoT projects using Raspberry Pi 5, Raspberry Pi Pico, and Python, Packet Publishing, 2024., el. ISBN:9781835088685

[3] D. D. Guinard; V. M. Trifa, Building the Web of Things: With examples in Node.js and Raspberry Pi, Manning, 2016. Electronic ISBN:9781617292682

[4] S. Budiyanto, L. M. Silalahi, A. R. Hakim, A. Hamid, D. Hanafi, "Vulnerability Analysis on Internet of Things (IoT) Networks using Raspberry Pi and Open Web Application Security Project (OWASP)," 2024 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE), Badung, Indonesia, 2024, pp. 58-63, https://doi.org/10.1109/FORTEI-ICEE64706.2024.10824490

[5] H. R. H. Hamid, M. A. I. b. M. A. Kamil and N. Y. Abdullah, "Portable Toolkit for Penetration Testing and Firewall Configuration", 2015, Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta, Indonesia, 2015, pp. 90-94, https://doi.org/10.1109/CyberSec.2015.26

[6] N. Kurniawati, A. Affandi, I. Pratomo and K. Gyoda, "Raspberry Pi-Based VoIP System For Rural Area," 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia, 2018, pp. 33-38, https://doi.org/10.1109/ISITIA.2018.8711237

[7] N. S. Ismail, N. A. Rashid, N. A. Zakaria, Z. I. Khan and A. R. Mahmud, "Low Cost Extended Wireless Network Using Raspberry Pi 3B+," 2020 IEEE Symposium on Industrial Electronics & Applications (ISIEA), Malaysia, 2020, pp. 1-4, https://doi.org/10.1109/ISIEA49364.2020.9188215

[8] T. Oda, M. Yamada, R. Obukata, L. Barolli, I. Woungang and M. Takizawa, "Experimental Results of a Raspberry Pi Based Wireless Mesh Network Testbed Considering TCP and LoS Scenario", 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), Fukuoka, Japan, 2016, pp. 175-179, https://doi.org/10.1109/CISIS.2016.86.

[9] M. C. Xenya, C. Kwayie and K. Quist-Aphesti, "Intruder Detection with Alert Using Cloud Based Convolutional Neural Network and Raspberry Pi," 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA), Cape Coast, Ghana, 2019, pp. 46-464, https://doi.org/10.1109/ICCMA.2019.00015.