The design of hardware firewall based on Acorn RISC Machine

Yunzhe Li, Xingfu Zhang, Bowen Jia*
College of Information Engineering, Wuhan University of Technology, Wuhan, Hubei 430070, China
*Corresponding author: jiabowen@whut.edu.com

Abstract. This article implements a high-performance and low-cost ARM firewall, which can guard computers under public network conditions and make public information more secure in today's information age. The designed firewall operates at the network layer to monitor the normal communication between the internal LAN and the external Internet, while resisting external network intrusions. The firewall can be configured to control whether internal hosts can access the Internet. When malicious Internet intrusion is detected, the firewall prevents data packets from flowing into the intranet.

1. Background
With the network power strategy, the national informatization development strategy, the national big data strategy, the "Internet +" action plan, and the further innovative development of China's digital economy, the network has shown a good development trend. The rapid expansion of cyberspace and its full penetration into all areas of society, the ever-increasing wealth, strategic value, and the deep dependence of the world's economic and social operations on it have made the overall security issue of cyberspace increasingly prominent. Cybersecurity has become another global public issue facing the international community. Issues such as user information exposure, cyber hacker extortion, and communication information fraud continue to occur frequently. Extortion worms named "WannaCry" and "Petya" successively appeared in May 2017. June and June raged the world, affecting many industries such as finance, energy, and medical care in more than 150 countries, making government and corporate institutions pay more attention to the potential risks of their own network security. [1]
Generally, firewalls can be divided into software ones and hardware ones. Software firewalls are easily setting, but are easily affected by the network and are prone to packet loss. When the network conditions are poor, the firewall's capabilities are severely restricted. In addition, the use of the software firewall not only occupies valuable system resources, but the network communication efficiency is not high. Moreover, it relies seriously on the host operating system and is lack of stability. Although the hardware firewall solves the problem of easy packet loss and other problems of software firewall, it has a long development cycle, consumes a lot of money, and has poor flexibility and is not easy to popularize.

The investigation of ARM-based firewall provides a novel path solve the deficiencies above the border firewall. By extending the security protection system of the firewall to each host in the network, on the one hand, it can effectively ensure that the user’s investment will not be high, and on the other Security brings comprehensive security protection. ARM firewall combines the advantages of software firewall and hardware firewall, and optimizes their shortcomings. It is foreseeable that as people pay more attention to network security issues, ARM firewall will have a good market prospect and development space. [2] In this work, the firewall can be configured to control whether internal hosts can access the Internet. When malicious Internet intrusion is detected, the firewall prevents data packets from flowing into the intranet.

2. The general design of embedded firewall
The embedded firewall can distribute the intrusion prevention function to individual PC, notebook and server in the network. Embedded firewalls distributed throughout the corporate network allow users to easily access information without exposing network resources to potential illegal intruders. The overall structure of the embedded firewall is shown in Figure 2. [3]
can also connect to EFW, get the protection of the embedded firewall and get permission to access the internal resources of the enterprise. However, the use of embedded firewalls does not mean that the traditional border protection wall is completely abandoned. The border firewall can be used as the first external barrier of the internal network to resist a large number of external attacks outside the internal network. It does not need to be placed inside and then resist it, which can reduce the data traffic of the internal network and the work of EFW. Therefore, in practical applications, a combination of the two can be used to obtain higher safety performance.

In short, this project will design and implement an embedded firewall with security, transparency, reliability, scalability, high performance and low cost.

3. Embedded firewall hardware design
Based on the previous analysis of the functions and characteristics of embedded firewalls, combined with actual needs, this article gives the following overall framework of embedded system hardware.

The embedded firewall hardware of this project adopts modular design and is divided into four modules: storage module, Ethernet interface module, JTAG and serial port debugging interface module, and peripheral circuit module. As shown in Figure 3.

![Figure 3. Hardware modular design.](image)

4. Embedded firewall software design
On the basis of hardware design, each part of the overall software framework of the embedded firewall is refined, as shown in Figure 4.

It can be seen from Figure 4 that the design of the overall software framework of the embedded firewall takes the embedded operating system as the core, the Bootloader is started by Flash, and is responsible for the initialization of the hardware device; the network card driver realizes the interaction with the physical transmission medium, and the application realizes various functions of embedded firewall. Bootloader, operating system and network card driver are the basic software of the embedded firewall. On this basis, write or transplant application programs to realize the function of the firewall.

By the design of the overall framework of embedded firewall software, the software layer can be clearly divided into four modules: Bootloader, embedded operating system, network card driver and application program. These four modules are related. Figure 2.6 is the working sequence diagram of these four modules. First, the Bootloader initializes the hardware device and establishes a map of the
memory space to prepare a correct startup environment for the final call of the embedded operating system kernel; then the operating system loads the driver to enable EFW to receive and send data packets; then the operating system calls the application. The program processes the received data packets and returns the processing results; finally, according to the processing results of the application program, the operating system calls the driver to send the data packets allowed to pass. The design of these four modules is described in detail below.

(1) Bootloader is a small program that runs before operating system kernel or user application program. Similar to the BIOS in the PC and the MBR boot area in the hard disk, it is used to complete the transition from hardware boot to operating system, realize the initialization of hardware devices, stack settings, memory space mapping, and set CPU registers to appropriate states. Call the kernel of the operating system to be ready. Bootloader is closely related to the hardware system and has a strong dependence on hardware. Therefore, it is not possible to establish a universal general Bootloader. Only the correlation between them can be used to establish a Bootloader "template". Templates are customized and transplanted to design and implement the required Bootloader.

(2) The embedded operating system is the control center of the embedded system's software and hardware resources. It organizes multiple users to share various resources of the embedded system in a reasonable and effective way as possible. The so-called reasonable and effective method refers to how the operating system coordinates and makes full use of hardware resources to achieve multitasking. Another feature of embedded operating systems is that for different platforms, the system is not directly usable, and generally requires a transplanted operating system for a specific platform to work normally.

(3) The embedded operating system supports three types of hardware device driver types: character devices, block devices and network devices. In this project, the hardware design knows that the network device driver needs to be written. The network device driver module is in the lower layer of the network subsystem of the operating system kernel, and directly operates the hardware device.
(4) The application program belongs to the functional module of the embedded firewall, and the application program is written according to the different functional requirements of the firewall. The application program of this project can be roughly divided into three parts: basic packet filtering module, application layer filtering module and content filtering module to enhance the function of EFW.

5. Conclusions and prospects
In view of the ever-developing network technology and frequent network attacks, whether it is individuals or enterprises, ordinary users or the establishment of databases, different levels of firewalls are required to filter and filter data. For ordinary individual users, since they are basically not subject to targeted network attacks, ordinary software firewalls are sufficient to meet their needs. However, for some small LANs, such as campus networks and home sharing networks, the risk of being attacked is greater. If a hardware firewall is used, not only the content that needs to be protected is too rigid, it is impossible to increase or decrease functions according to user needs, and the cost is also makes the benefits of the firewall far less than its value. The software firewall needs to provide its computing power by the user itself. When there are more users connected to the network, its demand for computing power will place a greater burden on the server, occupying the resources that should be served to the user, and causing the card Pause and user experience decline.

Based on the above reasons, in the market environment where major companies mainly launch professional hardware firewalls for enterprise users and software firewalls for individual users, the market for small and medium LANs has not yet fully formed, resulting in a large number of users. Demand.

In the face of market gaps, this project designed a firewall system based on external hardware to transfer the filtering function of the firewall to external hardware. Users only know the detection information and can change the firewall configuration in real time according to the provided information and their own needs. Ensure data security without occupying computing power. This is a very attractive project.

Acknowledgements
This work was supported by “Independent innovation research fund project of Wuhan University of Technology”

References
[1] Hong Xiaojian. On the application of computer network security and defense measures [J]. Computer CD-ROM Software and Application, 2013, 16(02):181-182.
[2] Zhang Shuai, Jia Ruchun. Design and implementation of embedded firewall based on ARM11 [J]. Laser Magazine, 2018, 39(09): 166-170.
[3] Ge Guangchao. Research and implementation of embedded firewall [D]. Nanjing University of Aeronautics and Astronautics, 2006.