Design and Research of Firewall System of Communication Department Based on Network Information Technology

Xing Wang¹*, Tao Zhao¹

¹Jinzhou power supply company of State Grid Liaoning Electric Power Co., Ltd, China

*Corresponding author e-mail: wangxing@sgcc.com.cn

Abstract. In the past, the structure of traditional firewalls was similar to that of checkpoints, and the design structure was relatively simple. At the same time, it is also convenient for subsequent maintenance. As an isolation technology, it can be accessed by people with consistent identity information. But for some relatively high-level data information, using traditional firewalls, foreign intruders can easily obtain relevant information. This article chooses to use the working mechanism of network information technology, and then analyzes the hardware structure of the firewall based on the IPX2400 processor. Finally, a preliminary design of a firewall system for the communications department based on the IPX2400 processor is implemented, and its packet filtering function is realized.

Keywords: Network Information Technology, Data Plane, Control Plane

1. Introduction

Traditional firewalls mainly include packet filtering firewalls, application proxy firewalls, and monitoring modules. The Linux system also uses a modular design to facilitate its future expansion [1-2]. The packet filtering detection data packet mainly includes the data part and the end, it ignores the information content in the packet [3]. Among them, the header information includes address, destination address, encapsulation protocol, and output port interface [4-5]. The packet filtering firewall will make a decision to allow or disallow each packet according to the matching rules [6]. The function of the address conversion module can realize static network address conversion, port redirection conversion, etc. The firewall system is divided into web management, conversion, and kernel modules. In hardware design, considering the system components, it is necessary to reduce the hardware convexity [7-8]. In the design system, the Linux core and file system are written into Flash to avoid the transfer of hardware information and improve execution efficiency [9-10]. The identity authentication module mainly serves the internal network client, the user can realize data communication through authentication, otherwise the client needs to resend the request. In the design of the network address translation module, it is necessary to establish the mapping relationship, query the conversion stage, and release the mapping relationship after the operation is completed [11].

Intel is the leader in the development of network information technology, and the network information technology IXP2400 is one of the representative products in the second-generation
network information technology series developed by Intel. There are 8 micro-engines in each IXP2400, and each micro-engine contains 8 hardware threads. The instruction system of the microengine is specially optimized, and each instruction can be completed in one instruction cycle. The internal multi-threaded parallel working mechanism of the micro-engine and the parallel working mechanism of multiple micro-engines can improve the data processing capability of the IXP2400 network information technology to a considerable extent. The function of the firewall is realized through three ports. It uses two independent network cards, one is mainly for the security of the server, and the other is for data exchange. The implementation of the firewall proxy system can ensure the safe transmission of user information. The operating system it uses is embedded, which is convenient for modification and tailoring, and has a relatively high security performance.

2. Firewall structure

2.1. Firewall hardware structure

The firewall system of the communications department consists of a firewall with IXP2400 network information technology and a computer for remote control of the firewall.

The firewall host containing the IXP2400 network information technology is the main body of the firewall system of the communications department, which is mainly composed of two IXP2400 chips (namely Ingress and Egress) and storage devices (DRAM, SRAM), and an IXD2410 external network card. The core component of the firewall host is the IXP2400 network information technology. The network information technology chip is composed of 8 micro-engines (divided into two groups), SRAM controller, DRAM controller, Xscale Core, SHaC, and MSF (Figure 1).

Figure 1. Firewall hardware structure

The firewall host receives data packets from the IXD2410 external network card through the MSF.
chip, completes network address translation, virtual private network on the IXP2400 chip (Ingress), and performs packet filtering on the third and fourth layers of the data packet (including state detection). After that, the data is transferred to another IXP2400 chip (Egress) through the internal communication protocol, and this IXP2400 chip (Egress) completes a series of tasks such as adding a second layer header, queuing, and sending.

The computer used for remote control of the firewall can provide functions such as remote control, log storage and analysis for the communication department's firewall system.

2.2. Firewall system structure

(1) Software structure design

The software of firewall based on network information technology can be divided into two layers: Data Plane (also called data highway or lower layer in some places) and Control Plane (also called core control plane or lower layer in some places). Upper floor) (Figure 2).

![Figure 2. Firewall system structure](image)

What is the data plane? Running on ME that supports hardware multithreading, the system hardware provides support, scheduling, and resource management. The combination of program codes is the data plane. Programs in the data plane can directly access almost all hardware resources used in the entire system. High-speed processing and forwarding of ordinary data packets is the basic function of the data plane. Data packets passing through the firewall system of the communications department will be received by the data plane first. The data plane needs to determine whether it can be processed, and discard the data packets that cannot be processed later. If there is a data packet, although the data plane cannot process it, but the control plane can process it, the data plane will be delivered to the control plane according to the processing needs. In fact, most of the data passing through the firewall only needs to be processed by the data plane, and only a small amount of data packets need to be delivered to the control plane.

What is the control plane? The control plane is a combination of program codes running on the XScale Core processing chip. Since the data plane needs to forward massive data packets on the network at a high speed, in order not to affect the performance of the firewall, when the data plane receives some small but troublesome application layer data packets, the processing speed is slow and it takes a long time. The data packets are sent to the upper control plane for independent special
processing. At the same time, the control plane can also provide a simple and easy-to-use system management and performance monitoring platform for firewall system administrators.

The data plane mainly implements functions such as abnormal data packet processing, packet filtering, and NAT, and the control plane mainly implements functions such as packet filtering core, NAT core, VPN, URL filtering, configuration management, and logging. The control plane can be further divided into three parts according to different functions: the control part, the management part and the corresponding part of the data plane module.

After the data packet preprocessing micro-block group detects abnormal data packets, according to the type of abnormal data packets, the data packets are sent to the VPN module, URL filtering module and other modules of the control plane for corresponding processing. The processed data packet is sent back to the pre-processing micro-block group of the data plane, and the pre-processing micro-block group is handed over to the processing micro-block group. After the processing micro-block group receives the data packet, it is processed by the packet filtering micro-block and the NAT micro-block.

The abnormal data packets sent from the data plane will be sent to the control plane, and corresponding processing will be carried out according to the different types of data packets. This part mainly includes the fragment reassembly module, URL filtering module, and VPN module; data plane micro-block correspondence The part is mainly for the two micro-block groups on the data plane: packet filtering micro-blocks and NAT micro-blocks, which provide a series of initialization tasks, data management tasks, memory management tasks, etc., which are required. This part mainly includes packet filtering core modules and The two NAT core modules; the management part is mainly for the necessary management of the firewall system of the communication department, inputting the filtering rules of the firewall from the control computer, configuring the firewall, managing the filtering rules used, and recording the abnormal conditions of the firewall. This part mainly includes the configuration Management module, log module.

(2) Data graphic design

The data plane works on the micro engine and is the main level of data processing. The software on the IXP2400 micro-engine is divided into multiple micro-blocks according to different functions. What is the so-called microblock? They are individual microcode functions with relatively independent functions, and a single microblock can perform part of the data packet processing function. Multiple microblocks can be connected into a microblock group through the dispatch loop program of the system. Only one microblock group can run on each microengine, but a microblock group can run on one microengine Or multiple micro-engines, then, how do the micro-engines of network information technology communicate? They communicate through the resources provided by the system: scratchring, neighbor register (NNR), and shared memory (Figure 3).

![Figure 3. Data plane software structure](image)

1) RX micro-block group: After receiving the mpacket from MSF and reorganizing the complete data packet, a series of information related to the current data table is passed to the next-level data packet preprocessing micro-block group.

2) Pre-processing the micro-block group: In order to improve the overall efficiency and usability of the firewall, a micro-block group is prepared before processing the micro-block group. Carry out the MAC and IP binding check of data packets, and send fragmented packets, VPN packets, and data packets requiring URL filtering to Xscale processor for specific processing.

3) Processing micro-block group: responsible for static packet filtering, dynamic packet filtering, DNAT, SNAT, routing query and other functions. Most of the data packets are processed in this micro-block group.

4) Queue Manager module group: This is a drive module that runs on a separate micro-engine and is responsible for using the Q-Array hardware structure in the SRAM Controller to perform enqueue and dequeue operations on the sending queue.
5) TX micro-block group: receive a data table from QM after dequeue operation, then split the data packet into multiple mpackets, then move mpacket into TBUF, and finally send mpacket through the sending state machine in MSF Go to the communication network.

3) Control plane design

The control plane works on Xscale. The control plane is mainly responsible for processing abnormal data packets and special data packets that cannot be processed by the data plane. The control plane is also responsible for the management and configuration of the firewall, log records and other management functions.

The software on Xscale is organized in the form of Core Componet (CC). The development of the core components is carried out by using the Resource Manager API (resource manager interface) and CCI library in IXA Portability Framework. The core component and the microblock on the data plane coordinate their work to complete the data packet processing task together. The core component and the microblock have a one-to-one or one-to-many relationship, and the core component is responsible for processing abnormal data packets and special data packets uploaded by the corresponding microblock.

For example: the VPN encrypted data packet detection microblock on the data plane, after detecting the VPN encrypted data packet, the corresponding information of the data packet needs to be sent to the VPNNCC of the control plane, and the VPNNCC of the control plane decrypts the data packet, and then VPNNCC sends the decrypted data packet to the data plane for subsequent processing. After the processing is completed, the VPN data packet encryption microblock is sent to the VPNNCC of the control plane, and the VPNNCC performs encryption and other processing again before sending to the destination host.

The specific functions of each module of the control plane are as follows:

1) VPNNCC: Decrypt the VPN encrypted data packets sent by the data plane VPN encrypted data packet detection microblock, and encrypt the filtered VPN data packets sent by the data plane VPN data packet encryption microblock.

2) Fragmentation and reorganization CC: Fragmentation and reorganization of the fragmented data packet sent from the data plane, restore it to a complete data packet, and then send it to the data plane for subsequent processing.

3) URL filtering CC: Perform URL address filtering and keyword filtering on data packets sent from the data plane, and send the filtered data packets back to the data plane for subsequent processing.

4) Packet filtering core: Initialize the packet filtering micro-blocks of the data plane when the firewall is started, modify the configuration of the memory during operation, clean up the memory at the end, save necessary information, etc.

5) NAT core: when the firewall system of the communications department starts, it helps the NAT module on the data plane to perform necessary initialization work, modify the memory configuration during the operation of the firewall system of the communications department, and clean up when the firewall system of the communications department ends. Memory, and save necessary information, etc.

6) Configuration management CC: Once the administrator modifies the existing filtering rules of the system through the configuration management function of the character interface or graphical interface, or the administrator configures the entire communication department firewall system, the system needs to regenerate the rule table file Or the configuration file of the firewall. The configuration management module must update the data in the memory for the corresponding module as quickly as possible. At the same time, the configuration management module must also notify the log module that the administrator has made a new configuration and needs to be recorded in the database.

7) Log CC: If some CCs in the control plane encounter some special circumstances and need to record, then these CCs must notify the log CC to record for the administrator to check. Due to the limited storage space on the firewall, the log CC is recorded for a period of time, and the log records
need to be sent to the database of the remote host for unified management.

3. Realization of packet filtering function

All packet filtering micro-blocks are run on the four micro-engines of the second in group 0, the third in group 0, the zero in group 1, and the first in group 1. Since there are 8 hardware threads in each micro-engine, these four micro-engines have 32 hardware threads. These hardware threads are organized in a pipeline-like manner in a certain order.

Those codes running on the microengine can be divided into initialization and scheduling loops. The initialization code is run only when the firewall system of the communications department is started. After the initialization, the program system will automatically enter an infinite loop.

Each thread processes a data packet separately. The processing of the data packet is logically divided into phase1-phaseN according to each memory read, and the memory read usually requires thread switching. Network information technology is Use this method to hide the memory access delay behind the instruction execution time.

The micro-engine hardware thread in network information technology is non-preemptive. If the current thread does not actively give up resources and enters the dormant state, then those threads in the ready state will not be able to obtain the execution permission, and cannot use the signal to wake up the dormant state. State the thread and let it enter the ready state.

```c
#if(defined(START_ME)&&(DL_NEXT_ME==START_ME))
signal_me_ctx1[DL_NEXT_ME,DL_SIG_WAKE];
#else
signal_me[DL_NEXT_ME,DL_SIG_WAKE];
#endif
```

The meaning of the above code is that if START_ME is defined and the value of DL_NEXT_ME is equal to the value of START_ME, then the next micro-engine No. 1 thread is signaled to wake; otherwise, the next micro-engine No. 0 thread is sent Signal to wake it up.

It is the hardware multi-threading technology of network information technology that optimizes the performance of the packet filtering module that requires a large amount of data processing, so that the firewall can meet the requirements of the gigabit backbone network.

4. Conclusion

Network information technology provides a new design and development platform for traditional network equipment such as firewalls. This article uses the advanced architecture of IntelIXP2400 network information technology to address the high performance of micro-engine hardware multi-thread parallel processing and Xscale processor for complex task processing. A multi-level and modular software framework design is proposed, which not only meets the functional requirements of network users for firewalls, but also meets the performance requirements. Under this system, a powerful and high-performance firewall system for communications departments has been realized.

References

[1] Butt, M. A. (2013). Communication information technology: academic role & responsibilities. International Journal of Computer & Distributed System, 2(2), 1-1.
[2] Chin, J. S. & Raftelis, M. (2012). Methods and apparatus to protect and audit communication line status, 2(5), 101-104.
[3] Clark, J. A. (2013). Secure processing of confidential information on a network.7(3), 5-8.
[4] Erumban, A. A. & Das, D. K. (2016). Information and communication technology and economic growth in india. Telecommunications Policy, 40(5), 412-431.
[5] Guruswamy, K. (2014). Platform for analyzing the security of communication protocols and channels, 23(5), 159-173..
[6] He, X. Chomsiri, T. Nanda, P. & Tan, Z. (2014). Improving cloud network security using the tree-rule firewall. Future Generation Computer Systems, 30(jan.), 116-126.
[7] Kim, H. C. (2014). Special issue: computer networks and communications in multimedia and
information technology. Recent Patents on Telecommunications, 3(1), 1-1.

[8] Li, G. (2017). Book review "analytics in smart tourism design"; Information Technology & Tourism, 17(3), 367-370.

[9] Quy, V. K. Nam, V. H. Linh, D. M. Ban, N. T. & Han, N. D. (2021). A survey of qos-aware routing protocols for the manet-wsn convergence scenarios in iot networks., 7(3), 309-322.

[10] Stenson, W. C. (2019). Bridging the gap of communication between faculty and the information technology services department. ProQuest LLC, 742, 708-716.

[11] Yang, L. Cheng, X. Ghogho, M. Ayanoglu, E. Huang, T. & Zheng, N. (2019). Guest editorial special issue on iot on the move: enabling technologies and driving applications for internet of intelligent vehicles (ioiv). IEEE Internet of Things Journal, 6(1), 1-5.