Indonesian Journal of Electrical Engineering and Computer Science
Vol. 10, No. 3, June 2018, pp. 1310~1318
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i3.pp1310-1318

An FPGA-based Network Firewall with Expandable Rule Description

Raya. K Mohammed[1], Yoichiro UENO[2]
[1]College of Information Eng., Al-Nahrain University Baghdad, Iraq.
[2]Department of Information Environment, Tokyo Denki University, Inzai-shi, Chiba, 270-1382 Japan.

Article Info

Article history:

Received Sep 16, 2017
Revised Nov 18, 2017
Accepted Mar 17, 2018

Keywords:

Firewall
FFGA
NetFPGA
Network Performance

ABSTRACT

With the rapid growth of communications via the Internet, the need for an effective firewall system which has not badly affect the overall network performances has been increased. In this paper, a Field Programmable Gate Array (FPGA) -based firewall system with high performance has been implemented using Network FPGA (NetFPGA) with Xilinx Kintex-7 XC7K325T FPGA. Based on NetFPGA reference router project, a NetFPGA-based firewall system was implemented. The hardware module performs rule matching operation using content addressable memory (CAM) for higher speed data processing. To evaluate system performance, throughput, latency, and memory utilization were measured for different cases using different tools, also the number of rules that an incoming packet is subjected to was varied to get more readings using both software and hardware features. The results showed that the designed firewall system provides better performance than traditional firewalls. System throughput was doubled times of the one with Linux-Iptables firewalls.

Corresponding Author:

Raya. K Mohammed,
College of Information Engineering,
Al-Nahrain University Baghdad, Iraq,
Email: rayakhahtan@coie-nahrain.edu.iq

1. INTRODUCTION

As computer networking and the Internet are becoming more and more demanded in all over the world, computers and local area networks became more vulnerable to attacks as long as it is very common for them to be connected to the Internet [1].

For this reason, the need for enhanced network security system with high performance is being increased. A firewall is a network security system that prevents unauthorized access from passing through the network. It works as a barrier placed between the local network and the outside world to regulate the flow of traffic [2]. The main function of the firewall is to examine every incoming and outgoing packet passing through it and decides whether to accept or deny the packet depending on its designed rules [3].

A firewall can be a software application or a hardware device running on a computer or a network to block any unauthorized access while permitting the authorized communication [4]. As compared with software firewalls, a hardware firewall is higher speed, more secure and more convenient for a large number of user's networks. But however, it is more expensive, harder to setup and configures. Editing and maintaining the rule-set in traditional hardware firewalls become a problem when firewall rules are becoming larger [5,6].

This paper proposed a firewall system that incorporates the best features by adopting the good points of traditional hardware and software firewalls while minimizing the negative points of each. The implementation of the designed system was based on FPGA technology.

2. FPGA-based Proposed Firewall System

The complexity and processing time of the firewalls were initiated to increase when the size of its rule set is being increased. In this paper, the rules of the designed NetFPGA-based firewall system are very flexible and can be modified easily by any user at any time. An FPGA-based firewall can reduce the cost and complexity that required to secure a large private network. The design of this firewall takes on the best features of traditional hardware and software firewalls while minimizing or avoiding the negative aspects of each.

2.1 FPGA & NetFPGA

Because of an FPGA's ability to quickly map and re-map parallel hardware designs onto the same device, it's an excellent design platform [7]. An FPGA is a semiconductor device that its function can be defined after manufacturing. FPGAs are efficient choices in applications where high-performance computing is required such as financial, medical imaging, etc. An FPGA contains a regular structure of the logic cell and interconnections which are under the designer's complete control, which means that the designer can design, program and make changes to the designed circuit at any time [8,9]. A NetFPGA is an FPGA-based open platform. NetFPGAs enable designers and researchers to build high-speed, hardware-accelerated networking systems. They are line-rate, flexible and open source hardware and software platforms used for research, teaching, and networking components development. The NetFPGA environment includes boards, reference projects, and software tools. NetFPGA board is a hardware accelerator built with FPGA driving 1/10/100 Gb/s network interfaces. There are four NetFPGA boards : NetFPGA-1G, NetFPGA-10G , NetFPGA-CML, & NetFPGA-SUME [10-12].

This work deals with the NetFPGA-1G-CML (shown in Figure 1) which enables rapid prototyping of networking devices. Its FPGA hardware is a Xilinx Kintex-7 325T.

Figure 1. NetFPGA-1-CML boar

The designed firewall is based on modifying the NetFPGA-1G-CML Reference Router Project. The implemented firewall system is a hardware and software co-design in which main software design was built using C programming language while the main hardware blocks were built using Verilog HDL. The whole design has been implemented and evaluated on NetFPGA platform with Xilinx Kintex 7 - XC7K325T on NetFPGA-1G-CML board. Some operations of the firewall are processed in hardware while others are processed in software.

2.1.1 NetFPGA Reference Router

One of the reference projects of NetFPGA platform is an IPv4 router which was used in this work. The NetFPGA reference router forwards packets from all four 1Gbps interfaces on the card simultaneously. The routing information and interface addresses are configured from the host at the runtime. The project includes the software packages and hardware design which had been designed based on Verilog HDL. The main software component of the NetFPGA reference router is called SCONE (software component of the NetFPGA). It is a user-level router that performs IPv4 forwarding and handles Address Resolution Protocol (ARP) and various Internet Control Message Protocol (ICMP) packets. SCONE had been designed so as to write a set of rules using C programming language. SCONE mirrors a copy of its MAC addresses, IP addresses, routing table, and ARP table to the NetFPGA card [13, 14].

2.2 Hardware Designed Firewall

The designed hardware firewall system performs the operations described in the flowchart shown in Figure 2.

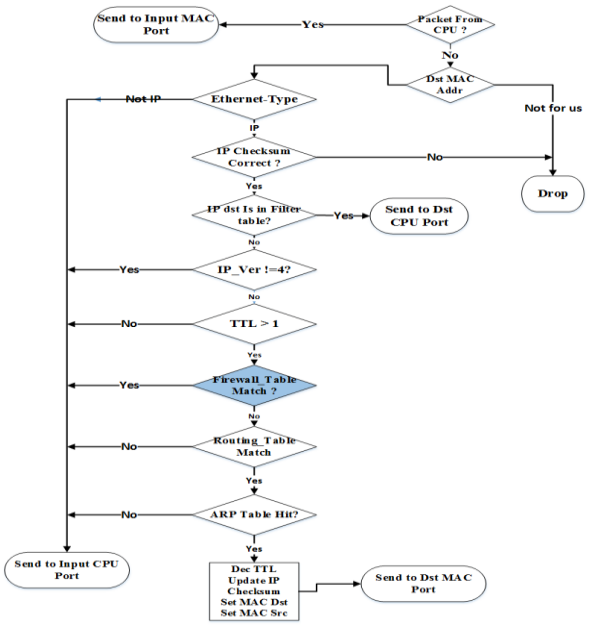

Figure 2. The designed firewall system operation

The function of the firewall module is to check the incoming packet destination IP address and compare it with the rules in the firewall table. If a match is found, a firewall_hit signal occurs, and the packet is sent to the software part of the firewall system. The latter checks other packet's header information and decide whether to accept or deny the packet according to the software rules. If no match is found, the packet is passed to the next modules for further processing.

The packet matching is performed using content addressable memory (CAM) of FPGA's on-chip which enables high-speed data searches [15]. Using Integrated Synthesis Environment (ISE) design suite, the Verilog source codes of the designed firewall system were synthesized. A schematic viewer for the firewall designed module is shown in Figure 3.

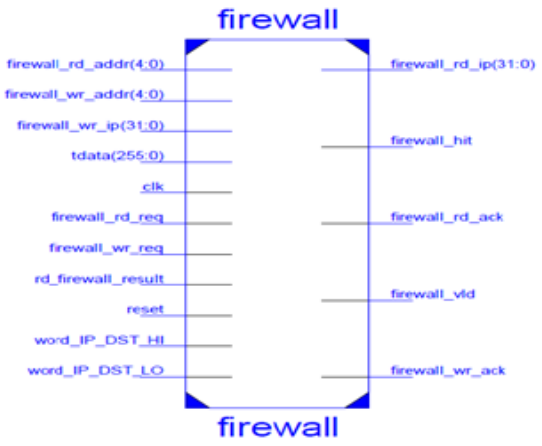

Figure 3. Designed firewall module structure

2.3 Software Designed Firewall

The firewall software part was designed using C programming language. It is based on the SCONE NetFPGA. A set of firewall rules is designed and inserted into this model. These rules are very flexible and can be modified easily by any user at any time.

An incoming packet arrives at this software part if its destination IP address matches an entry in the hardware firewall table. The software part detects the header information of the incoming packet. Further, it can display information of all packets while the software is running. Then the part compares the detected packet information with the rule and allows the packet to pass through the NetFPGA firewall and send it to the destination or drop it depending on the result from matching operation. In the software part, Java graphical user interface (GUI) and command line interpreter are also maintained for displaying, inserting and updating the firewall table, routing table, ARP cache.

3. Results and Analysis

For testing the NetFPGA-based prototype firewall system, the network shown in Figure 4 was configured.

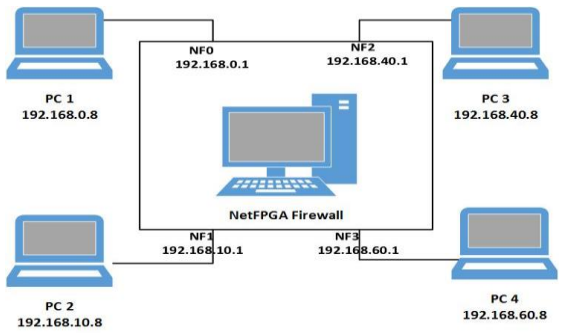

Figure 4. Networking test environment

The NetFPGA-1G-CML four Ethernet ports are (NF0, NF1, NF2, and NF3). First, IP addresses are assigned to the NetFPGA ports from the software part. Then, the 4 PCs are connected to the ports. PC1 with IP address 192.168.0.8 is connected to NF0 port with IP address 192.168.0.1. PC2 with IP address 192.168.10.8 is connected to NF1 port with IP address 192.168.10.1. PC3 with IP address 192.168.40.8 is connected to NF2 with IP address 192.168.40.1 while PC4 with IP address 192.168.60.8 is connected to NF3 port with IP address 192.168.60.1.

Firewall rules are written in the software firewall rule model. The IP addresses of the connected PCs are written onto the hardware part of the firewall by modifying the destination IP fields in the firewall table of the GUI. Examples of GUI output of the designed networks are shown in Figure 5 and Figure 6. The GUI of Figure 5 shows the general configuration of the firewall system which includes NetFPGA interface configuration, routing table, ARP cache, and firewall table while the GUI in Figure 6 shows the values of statistical variables which count the number of packets for different cases.

The last counter value (the number of packets sent to the CPU due to match in the firewall table) is high because all the PC's IP addresses are matched to the ones in the firewall table. This does not mean that all the packets will be dropped by the firewall because the packets are sent to the software firewall and then decided which packets should be passed or dropped.

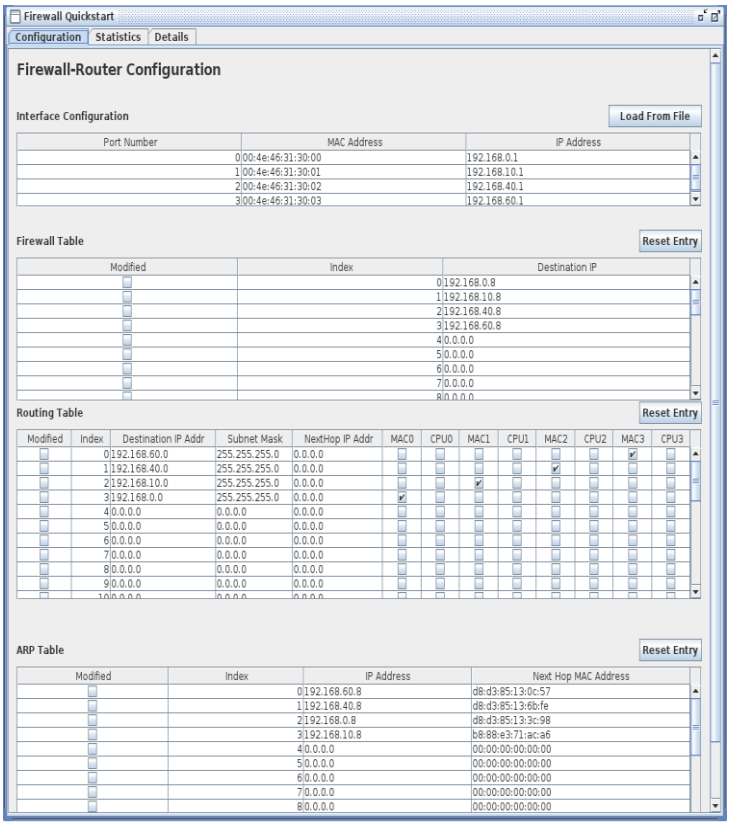

Figure 5. An example of GUI output of firewall configuration

Figure 6. An example of GUI of statistics variables

For throughput testing, PC3 in Figure 4 was configured as TCP server and PC1 as TCP client. Iperf network testing tool is used to measure system performance. The TCP bandwidth rate shown in Figure 7 confirmed that the developed NetFPGA-based firewall can provide a throughput of more than 900Mbps.

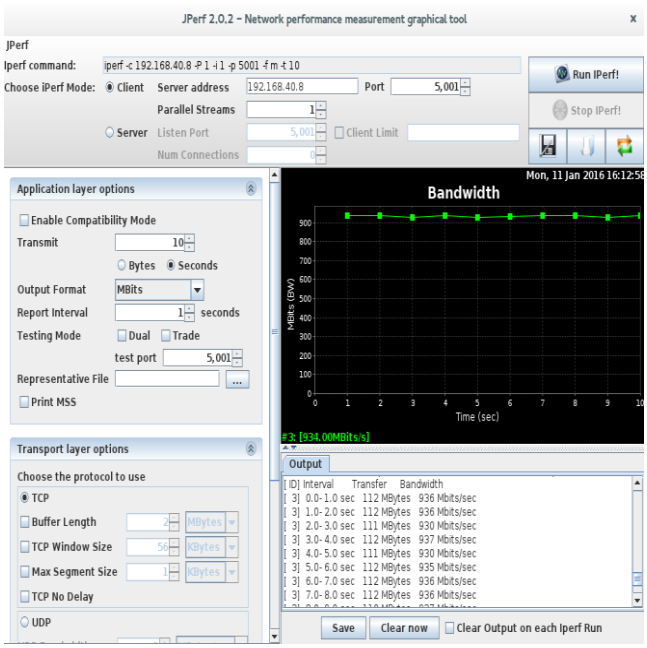

Figure 7. TCP bandwidth rate

3.1 Firewall Performance Test

For evaluating the NetFPGA-based firewall system performance, the network shown in Figure 8 was also configured. To perform bi-directional data transfer between the computers connected to the NetFPGA, PC-A with IP address 192.168.0.8 is defined as FTP client1 to PC-B FTP server1 and FTP server2 to PC-B client2. Furthermore, PC-B with IP address 192.168.40.8 is defined as FTP client2 to PC-A server2 and FTP server1 for PC-A client1.

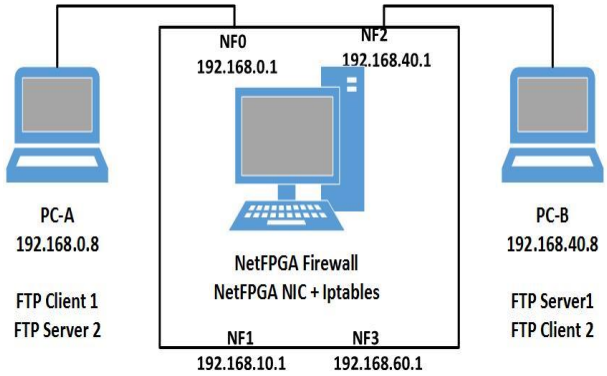

Figure 8. Firewall performance test example

For firewall performance comparison testing, the firewall package running on Linux (Iptables) is used. The first test was performed by programming the FPGA chip in NetFPGA board so as to function the firewall designed bitstream file; the NetFPGA works as NetFPGA firewall with its designed software and hardware parts. The second test was performed by programming the FPGA chip in NetFPGA board so as to function only a network interface card (NIC), using Ifconfig-commands in Linux to set the IP addresses to the NetFPGA ports. Linux Iptables was enabled, and firewall rules were added. In the second test, the NetFPGA works as NIC to Iptables software firewall. Table 1 shows the results of latency and memory usage in the two firewall types.

Table 1. Latency and Memory Usage Comparison

Firewall-type	Latency	Memory Usage
Linux-Iptables	0.717 ms	27.26%
NetFPGA-Based Firewall	0.402 ms	23.31%
Directly Connected	0.381 ms	---

Using FTP command line, different data size was transferring from PC-A to PC-B and from PC-B to PC-A. The bandwidth was also evaluated, and the results are shown in Table 2.

Table 2. FTP File Transfer Bandwidth Rate Comparison

Data	Firewall-type	Client	Bandwidth (Mbps)
2.2Mbytes	Iptables-Firewall	PC-B	198.786
	NetFPGA-based Firewall		437.382
	Iptables-Firewall	PC-A	214.844
	NetFPGA-based Firewall		592.031
236Mbytes	Iptables-Firewall	PC-B	182.228
	NetFPGA-based Firewall		259.750
	Iptables-Firewall	PC-A	163.326
	NetFPGA-based Firewall		455.018

The bandwidth rate comparison shown in Figure 9 was evaluated with 32 entries in the firewall rule for both the NetFPGA-based firewall and the Iptables-based firewall, i.e. 32 destination IP addresses were inserted into the firewall table of the designed firewall. Furthermore, the same rules were inserted to the Iptables. In this test, the IP addresses of PC-A and PC-B did not match any entry in the firewall table for both cases.

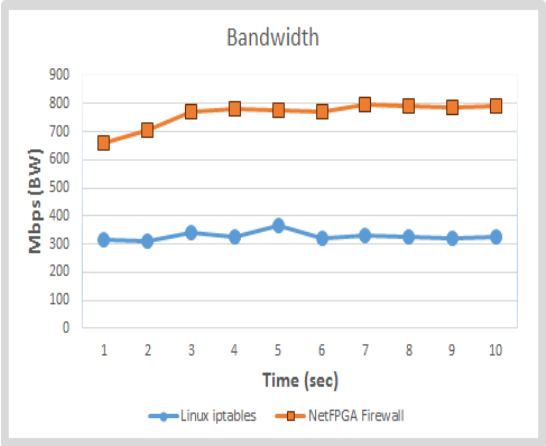

Figure 9. Bandwidth Comparison between Iptables and NetFPGA Firewalls without Rule Match

Another test was performed by inserting the IP address of PC-B in the firewall table for both NetFPGA-based firewall and Iptables-based firewall. The bandwidth rate comparison for this test is shown in Figure 10. The firewall performance is in lower speed as compared with the evaluation shown in Figure 9 because the packets had been sent to the software part of the firewall.

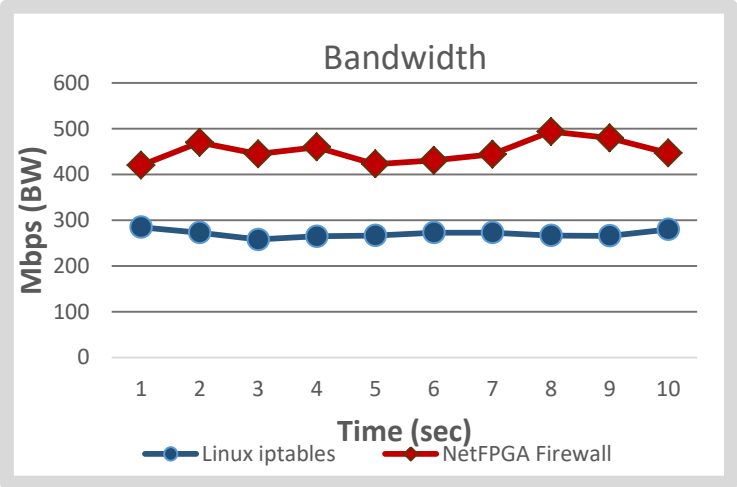

Figure 10. Bandwidth Comparison between Iptables and NetFPGA Firewalls with Rule Match

4. CONCLUSION

In order to provide higher network security, it is important to use an efficient firewall system which has little or no affecting overall network performance. Through this study and research experience, we can conclude that some traditional firewalls provide a higher level of security, but they may affect traffic loads and network throughput and latency since packets must be compared against complex firewall rule tables. Other firewalls, which may have less effect on network performance, cannot provide the same security level. For these reasons, this research focused on developing a new firewall system that can strongly protect networks and has a minimal effect on network performance. The developed firewall system is a hardware and software co-design. As comparing with Linux Iptables-based firewall, it was confirmed that the developed NetFPGA-based firewall can provide better performance. It can provide the double throughput of the Linux Iptables-based firewall. As a future work, it is expected to develop the hardware part performing all packet processing. The software part can also be developed to perform more complex operations such as examining and changing the actual contents of the packet rather than examining packet's header information. If this work would succeed, a firewall with excellent performance will be realized

REFERENCES

[1] Alfan Presekal, Riri Fitri Sari. "Performance Comparison of Host Identity Protocol and TCP/IP with Firewall against Denial of Services." *TELKOMNIKA Indonesian Journal of Electrical Engineering.* Vol. 12, No. 12, December 2014, pp. 8335 - 8343.

[2] Jad Naous, Glen Gibb , Sara Bolouki, Nick McKeown. "NetFPGA: Reusable Router Architecture for Experimental Research."*The ACM workshop on Programmable routers for extensible services of tomorrow*.2008.

[3] Mohamed Yousuf Hasan, Poornima V.P, Sujendran S, Karthikraja D. "FPGA Based Firewall using Embedded Processor for Vulnarability Packet Detection." *International Journal of Reconfigurable and Embedded Systems (IJRES).* Vol. 3, No. 1, March 2014, pp. 31-38.

[4] Ayla Hasanalizadeh-Khosroshahi, Hossein Shahinzadeh. "Security Technology by using Firewall for Smart Grid." *Bulletin of Electrical Engineering and Informatics.* Vol. 5, No. 3, September 2016, pp. 366-372.

[5] S. Ezzati, H. Reaza, A. Chegini, P. HabibiMehr. "A New Method of Hardware Firewall Implementation on SOC." *IEEE International Conference for Internet Technology and Secured Transactions*. 2010.

[6] G.Jedhe , A.Ramamoorthy , K.Varghese. "A Scalable High Throughput Firewall in FPGA." *IEEE Symposium on FPGA for Custom Computing Machines*. Napa. 2008.

[7] MARYAM REZAEE. "*An FPGA Test-Bed to Demonstrate Deterministic Guaranteed-Rate Services in the Internet of Things*." MSc thesis. Canada: McMaster university, Electrical & Computer Engineering; 2015.

[8] Andrew Moore. "FPGAs for DUMMIES". *Hoboken: John Wiley & Sons. Altera Special Edition*. 2014.

[9] A.SVENSSON , J.FLOD. “System design of an FPGA and analog based point-to-point wireless link.” MSc thesis. Sweden: Chalmers University of Technology; 2014.
[10] Diego Reforgiato, Fabio Battaglia. “NetFPGA Architecture and Hardware Description.” Germany: LAP LAMBERT ACADEMIC PUBL.2012.
[11] Abhishek Dwaraki. “Hardware Implementation of Queue Length Based Pacing on NetFPGA.” MSc thesis. Amherst: University of Massachusetts, Department of Electrical and Computer Engineering; 2011.
[12] Glen Gibb, John W. Lockwood, Jad Naous; Paul Hartke; Nick McKeown. “NetFPGA – An Open Platform for Teaching How to Build Gigabit-rate Network Switches and Routers.” *IEEE Transactions on Education*. 2008: pages 364 - 369.
[13] Ahmed Khalid. “*High Speed NetFPGA Router*.” Germany: LAP LAMBERT Academic Publishing. 2012.
[14] R.Ajami, A.Dinh. “Design a hardware network firewall on FPGA.” *IEEE 24th Canadian Conference on Electrical and Computer Engineering*. 2011.
[15] Young H. Cho , William H , M. Smith. “Deep Packet Filter with Dedicated Logic and Read Only Memories.” *IEEE Symposium on Field-Programmable Custom Computing Machines*. Napa. 2004.