H/W BASED FIREWALL FOR HIGH-PERFORMANCE NETWORK SECURITY

Jong-Gook Ko, Ki-Young Kim and Keul-Woo Ryu
Electronics and Telecommunications Research Institute (ETRI)
1 Kajeong-dong, Yuseong-gu, Daejeon 305-350, Korea
Tel +82-42-860-5940, Fax +82-42-861-5611
{jgko, kykim, kwryu}@etri.re.kr

Abstract: Recently, enterprises, service provider, and e-businesses confront increasing security and performance challenges. Securing network, host, and on-line application is absolutely important. At the same time, security function must not disturb productivity. To ensure that increasing network traffic is safe and their networks are secure, these organizations must provide security with bias toward solutions that accommodate performance demands, while providing the security and networking features required to run their businesses. That is, best solutions are those that combine high performance with topnotch security. For satisfying those requirements, we have developed hardware based and high performance Security Gateway System (SGS) which providing security functions such Firewall, IDS, Rate-limiting, and Traffic metering in wire speed. In this paper, we especially describe how H/W based Firewall features are implemented in SGS.

Key words: Firewall, Network Security, Security Gateway System, packet filtering

1. INTRODUCTION

Today, Firewall among many security functions is essentially provided in all security system. It means that firewall is fundamental and important security function. When a network is connected to the Internet, its users are enabled to reach and communicate with the outside world. At the same time, however, the outside world can reach and interact with the network. In this dangerous situation, intermediate system can be located between the network

E. Nardelli et al. (eds.), *Certification and Security in Inter-Organizational E-Service*

and the Internet to establish a controlled link, and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the network or hosts from threats and attacks. In short, firewall builds blockade between an internal network that is assumed to be secure and trusted, and another network, usually an external network, such as the Internet, that is not assumed to be secure and trusted. The general reasoning behind firewall usage is that without a firewall, a network's systems are more exposed to inherently insecure Internet protocols and corresponding services, as well as probes and attacks from hosts elsewhere on the Internet. Firewalls filter the traffic exchanged between networks, enforcing each network's access control policy. Firewalls ensure that only authorized traffic passes into and out of each connected network. To avoid compromise, the firewall itself must be hardened against attack. To enable security policy design and verification, a firewall must also provide strong monitoring and logging.

Network speeds have increased faster and faster in the last several years. Some networks run at gigabit speeds today, while 100-megabit networks have been commonplace. Even Internet connectivity speeds have increased to the point where 100 megabits is common at hosting sites, and is also becoming feasible for large organizations. Recently, 1giga, 2.5giga, even 10giga interfaces are developed and on the market.

The firewall technologies required to control inbound and outbound traffic have not, until now, developed as rapidly as networking speeds. The most popular firewall appliances today rely on desktop PC hardware and are implemented in software based, which can limit their performance. High-performance firewalls must surpass these limitations, and should be capable of performing more that simple security duties.

In this paper, we describe hardware based firewall which providing security function and assuring high performance. The rest of this paper is organized as follows. Section 2 describes design and composition of hardware based firewall. Performance test results are contained in section 3. And Conclusion and future work are discussed in section 4.

2. SYSTEM DESIGN AND COMPOSITION

Hardware based and high performance Security Gateway System (SGS) provide security functions such as firewall, IDS, Rate-limiting, and traffic metering which are implemented on two FPGA (Xilinx Vertex II Pro) chips in each security board module. Security board also has embedded CPU MPC 860 that embedded Linux OS operating in. Total five security boards can be installed to SGS. Figure 1 depicts overall security board composition.

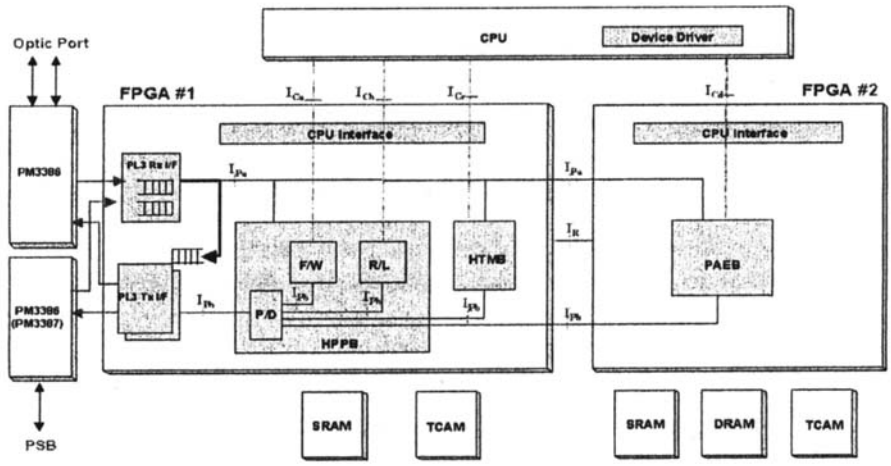

Figure 1: SGS secrity board composition

Firewall, Rate-limiting, and traffic metering are implemented in FPGA #1. and High Packet Processing Block(HPPB) in FPGA #1 consists of Firewall and rate-limiting. Each security board has two gigabit port interface. Firewall module has two kinds of sub-module. Figure 2 depicts firewall sub modules.

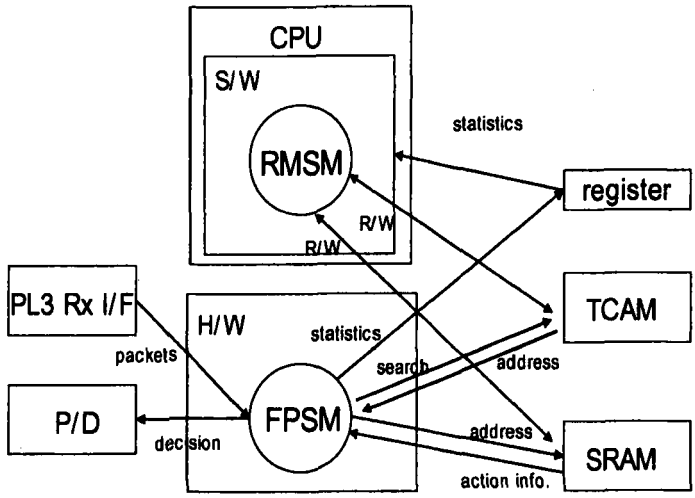

Figure 2 Design of firewall sub-modules

One is Filtering Process Sub-Module (FPSM) that is implemented on FPGA chip and the other is Rule Management Sub-Module (RMSM) that is software operating in embedded CPU.

2.1 Filtering Process Sub Module (FPSM)

FPSM makes decision whether the input packet should be permitted or dropped and is implemented using Verilog HDL. It uses one CYNSE 70256 TCAM for high speed rule searching and one SRAM to store action and statistic information. Each filtering rule match to action information in SRAM one to one. At first, FPSM receive input packets from PL3 Rx I/F and make key value for searching TCAM. Key value consists of Source IP, Destination IP, Source Port, Destination Port, Protocol, TCP Flags, ICMP header type, ICMP header code and so on. And FPSM get action information from SRAM using TCAM matching address founded by key value. Action information consist of 4 bits and are like following :

bit 0 : if set '1' => permit
bit 1 : if set '1' => block or drop
bit 2 : if set '1' => Forensic port #0 gathering
bit 3 : if set '1' => Forensic port #1 gathering

Both of bit 0 and bit 1 do not set at the same time but, others bits can be set concurrently. Statistic information on whether drop or permit are stored SRAM per filtering rules and those information are reported whenever user require.

Figure 3 depicts the processing of making decision whether the input packet should be permit or drop.

At first, if Key value of input packet does not matched to any rules in permission table, then the input packet is dropped. If matched to rule of permission, then it survey whether key value of input packet is matched to rules in blocking table again. If matched, the input packet is dropped but, if not matched, the packet is forwarded and copied.

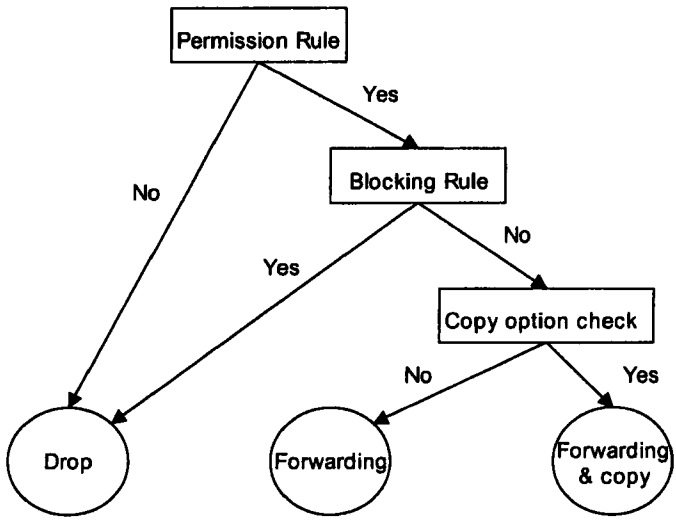

Figure 3: Processing of making decision

Permission Rule and blocking rule table are separated for effective filtering rule management. The reason why permission and blocking table are separated is not to make any conflicts between rules. For example, suppose that there are two kinds of rules like following and Rule 1 and Rule 2 applied at same table in order.

Rule 1 : Src IP (192.168.X.X) X means don't care
: Dst IP (210.123.10.12)
: Src Port (don't care)
: Dst Port (80)
: protocol (TCP)
Action => Drop
Rule 2 : Src IP (192.168.30.X) X means don't care
: Dst IP (210.123.X.X)
: Src Port (don't care)
: Dst Port (80)
: protocol (TCP)

Action => Permit

First match has priority in packet filtering matching. Accordingly, Packets which have source IP 192.168.30.X will be not permitted but blocked because the packet's key value matched to Rule 1. Manager can make rule properly that does not make conflict but, if there are thousands of rules, it's a heavy burden to manager.

TCAM capacity is 9Mbits (up to 128K entries in 72-bit configuration, up to 64k entries in 144-bit configuration) and is used for firewall and rate-limiting. So, only half of TCAM capacity is used firewall. For the filtering rule, 144-bit configuration should be used. Table 1 show TCAM address map for packet filtering.

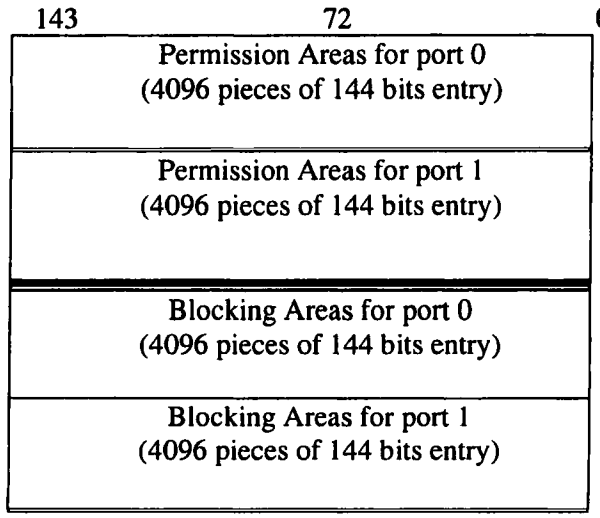

Table 1: TCAM address map for filtering rules.

2.2 Rule Management Sub Module (RMSM)

RMSM has the role of adding and deleting of filtering rules and has mirroring map of filtering tables in TCAM to manage filtering rules and also manage information of SRAM. Mirror map memory matched to TCAM address area is needed to manage filtering rules which are in hardware based TCAM because direct management of rules in hardware TCAM is restricted.

In case of adding new filtering rule, it should check whether the new rule is duplicated to already existing rule or not. If not, it finds empty entry area in TCAM mirror information in memory and add new rule to related location of TCAM and also add action information of new rule to related location of SRAM. When delete rule, it finds matched rule entry from TCAM mirroring information and delete entry in TCAM using index which gotten from

mirroring information. Rule updating is similar to deleting. Rule management procedure is like following:

```
rule_management(){
if(add){
 check whether already exists in mirror map;
 find empty entry of mirror map;
 add rule to TCAM using gotten index from mirror map;
 add action info. to SRAM using gotten index from mirror map;
 mirror map also added;
 }
If(del){
  check whether deleting rule exists in mirror map;
  if not founded, error message and go to exit;
  delete the rule in TCAM using gotten index from mirror map;
  delete action info. in SRAM using gotten index from mirror map;
  delete the entry in mirror map;
 }
}
```

Range matching and negation operation are also important in rule management because TCAM is basically exact matching device. In general, when manager make filtering rule, he may make port or IP range rules. Accordingly, one range rule should be divided to a large number of exact matching rules to support range matching. For example, port range from 1 to 3 can be transit to two rules that have port value binary "01" and binary "1x"(x means don't care bit) respectively. Separated permission and blocking tables are used for negation operation. For example, suppose that there is rule which drop packets except destination port 80 services. Then, the port 80 rule entry is added to permission table and the rule entry whose destination port field made by don't care is added blocking table.

3. EXPERIMENTAL RESULTS

We have used IXIA Traffic Generator/Analyzer to generate and transmit packet to SGS. Security board of SGS has two gigabit interface fiber ports and two ports are connected to IXIA Traffic Generator. One port is used to receive packets from IXIA and the other port is used to send packets to IXIA again after processing. Even though network bandwidth is gigabit, the actual bandwidth depends on packet size. Table 2 shows actual bandwidth on each packet size. Two kinds of tests, for blocking and permission, have been done

on three kinds of packet size. Filtering rules are also separated to 10, 100, and 1000 rules respectively.

Packet size	Actual bandwidth in Gigabit bandwidth environment
64 bytes	761 Mbps
256 bytes	927 Mbps
1500 bytes	986 Mbps

Table 2: Actual bandwidth on each packet size

At first, all blocking packets are generated and transmitted to SGS by IXIA. Table 3 shows that all packets are blocked regardless of the number of rules and packet size.

# of rules / packet size	10	100	1000
64 bytes	All blocked	All blocked	All blocked
256	All blocked	All blocked	All blocked
1500byte	All blocked	All blocked	All blocked

Table 3: Test results on blocking packets

Secondly, all accepting packets are generated and transmitted to SGS by IXIA. Table 4 shows that all packets are permitted regardless of the number of rules and packet size.

# of rules / packet size	10	100	1000
64 bytes	All permitted	All permitted	All permitted
256	All permitted	All permitted	All permitted
1500byte	All permitted	All permitted	All permitted

Table 4: Test results on permitting packets

Like test results, the number of rules has nothing to do with SGS system performance because Firewall is implemented in hardware. Actually, regardless of that the number of rules is 10 or 1000, TCAM rule searching is done from begin and end of TCAM address area.

4. CONCLUSION AND FUTURE WORK

In this paper, we have presented hardware based firewall for high performance network security. One of important requirements of security system is on high performance. Even though many security functions are supported, if not satisfied with network speed, those may not be used. We have developed security board which provides firewall function that support total 2 gigabit throughput (two gigabit ports).

Recently, most of firewall systems support not only static packet filtering but also dynamic packet filtering. Afterwards, we are going to add hardware based dynamic packet filtering.

References

[CZ95] Chapman, D. and Zwicky, E. "Internet Security Firewalls". O'Reilly, Sebastopol, Calf., 1995.

[Ken93] Kent, S. "Internet privacy enhanced mail". Commun. ACM 36, 8,(Aug. 1993),48-60

[Opp97] Rolf Oppliger. "Internet Security: Firewalls", Communication of the ACM, May,1997, Vol.40

[Wat02] "what to look for in next generation high-performance firewall appliances", www.watchguard.com, Nov. 2002.

[QVS01] Lili Qiu, George Varghese, Subhash Suri, "Fast firewall implementations for software-based and hardware-based routers", Proceedings of the 2001 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, Volume 29 Issue 1

[SML04] Schuehler, D.V.; Moscola, J.; Lockwood, "Architecture for a hardware-based, TCP/IP content-processing system", IEEE , Volume: 24 , Issue: 1 , Jan.-Feb. 2004 ,Pages:62 - 69