Indian Journal of Science and Technology, *Vol 8(25), DOI: 10.17485/ijst/2015/v8i25/80825, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Evaluation and Analysis of Network Firewalls in High Speed Networks

Jae-Kook Lee, Sung-Jun Kim*, Chan Yeol Park and Joon Woo

Korea Institute of Science and Technology Information, South Korea; jklee@kisti.re.kr, sjkim@kisti.re.kr, chan@kisti.re.kr, wjnadia@kisti.re.kr

Abstract

High speed and high capacity networks are critical for large scale (big) data services. In addition, security issues are even more important. KISTI (Korea Institute of Science and Technology Information) operates a variety of security facilities to provide secure supercomputing services to public users. A throughput of network firewalls affects entire trust networks. Because network firewalls act as the first line of defense against unwanted and malicious traffic flow between each networks. In this paper, we evaluate and compare the performance of two network firewalls are operated by KISTI in high speed networks and analyze results.

Keywords: High Speed Network, Network Firewall, Performance Evaluation, Security

1. Introduction

High speed and high capacity networks are critical for large scale (big) data services like computational science, nano physics, aerospace, and meteorology field. To support these services to public users, KISTI (Korea Institute of Science and Technology Information) operates the supercomputer. In Korea, first supercomputer (KISTI–1) was constructed in 1988. KISTI constructed KISTI–2 in 1997, KISTI–3 in 2002, and KISTI–4 in 2009. It is currently operating KISTI–4, which consists of shared-memory type GAIA 1 and GAIA 2 systems, and cluster type TACHYON 1 and TACHYON 2 systems (built in 2009)[1]. KISTI has been providing public computational resources to researchers using KISTI–4[2]. KISTI–4 has been connected KREONET (Korea Research Environment Open NETwork) which is providing a 10Gbps network speed. Figure 1 shows the volume of inbound traffic flows in the supercomputing service environment. Its maximum bandwidth is reached 1.1 GBytes/sec ($\fallingdotseq$ 8.8 Gbps).

KISTI also operates a variety of network security equipment to provide secure and stable supercomputing services to public users in gigabits speed network environment. These facilities are available 24x7, 365 days a year. In particular, network firewalls act as the first line of defense against unwanted and malicious traffic flow from internal to external network or from external to internal network. The sea-saw effect between firewalls and network performance is most concerning to network users; where strict security settings result in weak network performance and permeant security settings allow for a stronger one. Hence, evaluating firewall platforms and their impact on network performance is important when assessing the effectiveness of network security[3]. A firewall controls the incoming and outgoing network traffic based on applied access rule set. Rule sets are composed each specifying source addresses, destination addresses, source ports, destination ports, and an appropriate action. The action is typically 'accept' or 'deny'[4,5]. Network firewalls need to show robust performance because these firewalls are deployed in the front-end of trust network.

In this paper, we evaluate the performance of network firewalls (Cisco Catalyst 6509 with FWSM and Wins Sniper 10G Firewall) are operated by KISTI in high speed networks and analyze results to end-point servers.

The rest of this paper is organized as follows: Section 2 summarizes related work. Section 3 provides detail of performance testing environments and system specifications.

*Author for correspondence

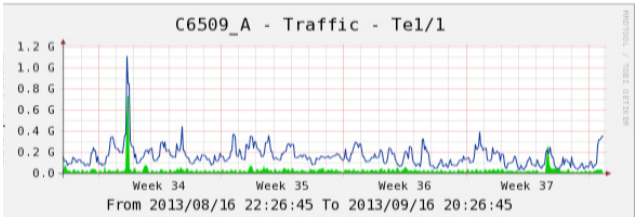

Figure 1. Inbound traffic on supercomputing service network.

Section 4 presents the results of firewalls performance evaluation. Finally, Section 5 concludes the paper.

2. Related Work

Many researchers published related works on firewall performance analysis. Most of the available work considered enhancing firewalls configuration management and detecting misconfiguration as presented in[6–9,11].

In[10] the researchers evaluated of firewall performance in gigabit-networks. They experiment the switch throughput, packet filtering throughput, packet filtering latency and cache efficiency on Cisco 5505 as firewall.

The researchers in[4] attempted to evaluate performance of major operational firewalls (Cisco ASA, Checkpoint SPLAT, and OpenBSD PF). The performance testing results clearly indicated that Cisco ASA provides better performance and Checkpoint SPLAT provides better functionality. OpenBSD PF also provides to be best open source solution if cost is the deciding factor. Checkpoint SPLAT provides better Firewall management with centralized policy management and better user interface than Cisco and PF. They proposed that Cisco ASA is one of the best choices for large corporate networks.

In[11] the authors presented an assessment methodology to analyze the performance of different firewalls platforms (Cisco ASA 5510 and Cisco Router 2811 with packet filter). The performance analysis considered delay, jitter, throughput, and packet loss. They showed that network-based firewalls outperformed personal firewalls in all metrics and Cisco ASA achieved better performance than packet filter.

3. Environment and Methods

3.1 Test Environment

In order to evaluate the performance of firewall, the testing environment install shown in Figure 2. As shown in

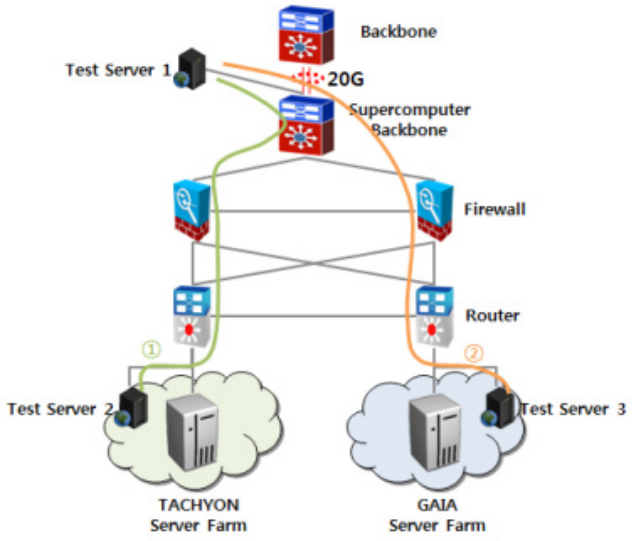

Figure 2. Experimental environment for firewall performance test.

Figure 2, the test-bed have one test server in the upper part of the supercomputer backbone and one server is installed respectively at the GAIA and TACHYON system sides located below routers. To compare two firewalls performance we change the firewalls in same environment.

All network sections were configured with 10Gbps network (except that the section connected to the backbone is configured with 20Gbps (10Gbps × 2)), and the specification of each device is listed in Table 1.

Two firewalls were used in the experiments: Cisco FWSM (Firewall Services Module) with ACE (FWSM) and Wins Sniper FW 10G (SniperFW) firewalls. FWSM is a high-speed, integrated firewall module for Cisco 6500 switches and provides the fastest firewall data rates: 5Gbps throughput. Up to four FWSMs can be installed in a single chassis, providing scalability to 20Gbps per chassis[12]. We use two FWSMs in this test. SniperFW is a high performance firewall with 10Gbps throughput[13]. Table 1 shows the specification of firewalls, test servers, and network switches that are used in the experimental testing. This network testing environment is the KISTI–4 network is currently operating by KISTI.

3.2 Measurement Tools and Methods

For the performance measurement tool, the widely used iperf[14] developed by NLANR/DAST, ftp, and wget[15], which are data transmission applications that use the FTP and HTTP provided for the supercomputing service, were used. For iperf, the bandwidth was measured by sending

Table 1. System specification

Systems	Specification
Test Server[1–3]	Dell Xeon Servers - Intel Xeon CPU 2.4GHz (24Cores) - 8GBytes RAM - GBIC : 10G Ethernet
Supercomputer Backbone	Cisco 7609 - GBIC : 10G Ethernet - Total Throughput : 720G
Firewall	Cisco Catalyst 6509 with FWSM / Wins Sniper FW 10G - GBIC : 10G Ethernet - Total Throughput : 6G(x2) /10G
Router	Force10 E1200 - GBIC : 10G Ethernet - Total Throughput : 100G/slot

packets to the client side after setting one test server as the server and the other as the client; for ftp and wget, the bandwidth was measured by sending an ISO file of 4 GBytes from one server to another.

TCP window size affects the measurement of the bandwidth that uses iperf. Figure 3 shows the change of bandwidth according to the size of the TCP window. On doubling the TCP window size from 64 Kbytes, the measurements increased up to 1 Mbytes. As shown in Figure 6, the TCP window size with the smallest standard deviation and highest average bandwidth in the current configuration is 512 Kbytes. When actually measuring firewall performance, the TCP window size was set to 512 Kbytes. The average bandwidth was set to the average of the results measured at least 30 times, excluding the minimum and maximum values, as shown in Equation (1), and the standard deviation was given by Equation (2).

$$\text{average} = \frac{\sum_{k=1}^{n} B_k - \left(B_{\max} + B_{\min}\right)}{n-2},$$
$$B_{max} = Max\left[B_1, B_2, \cdots, B_n\right],$$
$$B_{min} = Min\left[B_1, B_2, \cdots, B_n\right],$$
$$n = 30 \qquad (1)$$

$$\text{deviation} = \sqrt{\frac{1}{n}\sum_{k=1}^{n}\left(B_k - average\right)^2} \qquad (2)$$

4. Performance Evaluation

Figure 4 shows a graph of the measurement results (average) from the perspective of the GAIA system and Figure 5

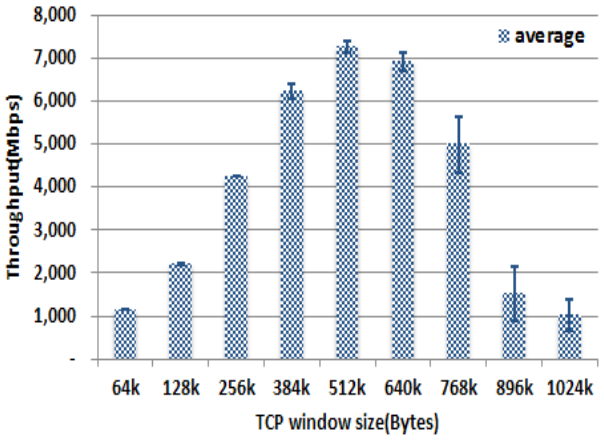

Figure 3. Average bandwidth by TCP window size.

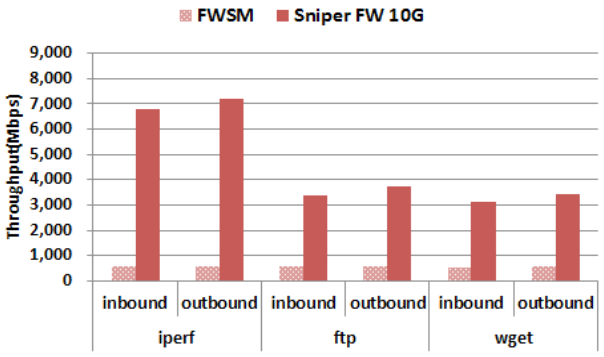

Figure 4. Network bandwidth on GAIA server farm (Test Server 1 ↔ Test Server 2).

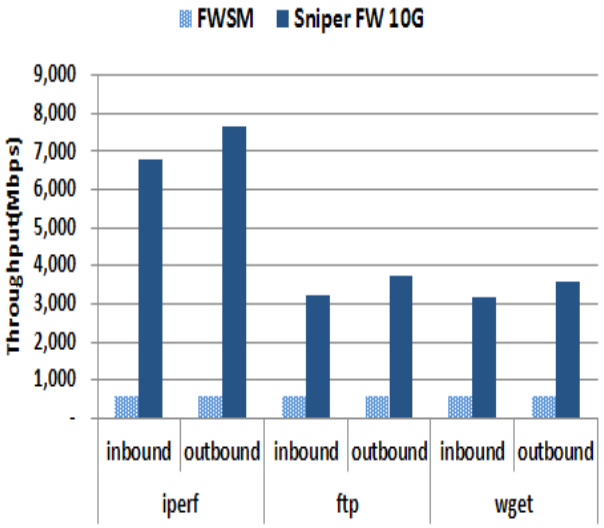

Figure 5. Network bandwidth on TACHYON server farm (Test Server 1 ↔ Test Server 3).

shows a graph of the measurement results (average) from the perspective of the TACHYON system. As shown in the two graphs, as compared with the inbound traffic from Test Server 1 to Test Server 2 or Test Server 3, the outbound traffic flowing in the opposite direction shows a higher performance. Furthermore, in the test using iperf, the overall bandwidth performance of FWSM is less than 1 Gbps, whereas that of Sniper FW 10G is 7 to 8 Gbps, i.e., 11 times better. In the test using the applications (ftp and wget), a bandwidth of 3 to 4 Gbps was recorded, which is approximately five or six times higher than that of FWSM

5. Analysis and Discussion

When the FWSM firewall is applied, performance at the end-point downs to less than 1Gbps. Table 2 lists the performance measurement result at the end-point when the firewall are applied. More detailed descriptions are provided in the next section for the environment, method, and result of the performance measurement.

The reason that performance (10Gbps) is not as expected when the firewalls are applied lies in the hardware architecture of the FWSM firewall, which is responsible for access control of the supercomputing service. Figure 6 shows the hardware architecture of FWSM[12].

The FWSM is connected to the backplane of the 6500 or 7600 through a full-duplex 6-gigabit Ethernet channel. KISTI operates the firewall with two FWSM modules (total 12Gbps). In this architecture, when traffic is sent from several source and destination systems, the firewall can guarantee full performance, but end-point users cannot be guaranteed a performance of over 1Gbps.

The reason the outbound bandwidth is higher than the inbound bandwidth in all cases of iperf, ftp, and wget is that the inbound traffic is slightly higher than the outbound traffic in the test conducted with the network

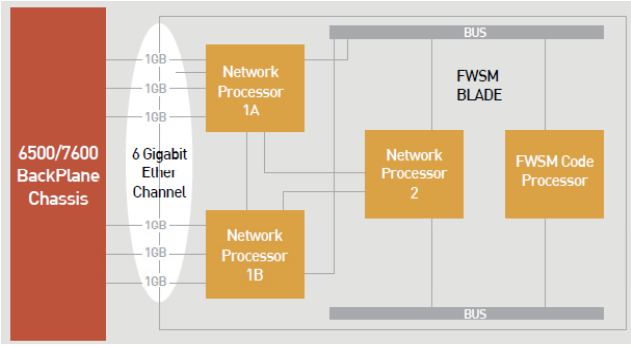

Figure 6. Hardware architecture of FWSM.

Table 2. Network traffic bandwidth when firewall is deployed

Systems	Direction	Bandwidth
GAIA	Inbound	901Mbps
	Outbound	908Mbps
TACHYON	Inbound	887Mbps
	Outbound	908Mbps

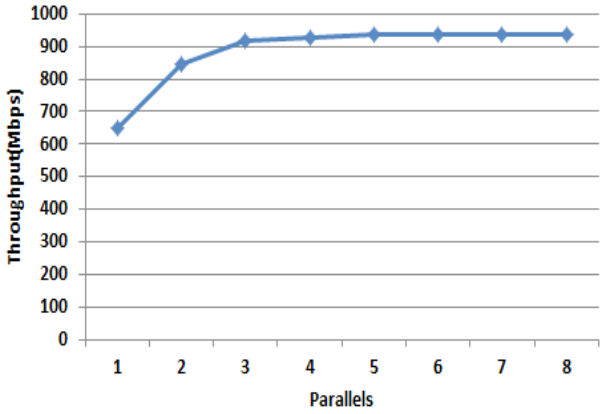

Figure 7. Bandwidth variation by multiple parallel streams.

actually operating. In addition, the performance measurement result using applications such as ftp and wget is lower than that using iperf because the transmitted files have to be read/written on a disk.

For FWSM, the throughput is 12 Gbps, but the test results confirm it to be less than 1 Gbps. With FWSM, the performance measured by increasing the number of sessions using the '–p' option of iperf is shown in Figure 7.

When one source/destination IP address is used, even if the number of sessions increases, the bandwidth does not exceed 1 Gbps. This is an FWSM hardware architecture problem, where the Gbps Ethernet of six channels operates in the backplane chassis. The performance is possible if traffic is sent simultaneously from many sources and destinations. In fact, increasing the number of test servers, as shown in Figure 8, confirms that the traffic processing bandwidth at FWSM could surpass 1 Gbps. However, performance at an individual test server, i.e., end-point, is less than 1 Gbps.

However, in the case of Sniper FW 10G, although it does not reach total throughput, a performance of 7 to 8 Gbps (iperf test results) is shown, even with one server. If fast data transmission is to be achieved using FWSM, the user has to disperse data in several servers and upload

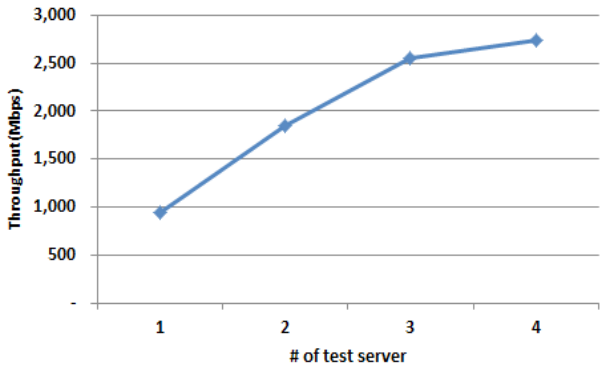

Figure 8. Bandwidth variation by multiple servers.

them to use the supercomputing service, and the calculation result has to be downloaded. This becomes an inconvenient factor for users. In contrast, in the case of Sniper FW 10G, when one user employs large bandwidth, it may affect other users. Nevertheless, in the case of Sniper FW 10G, a quota can be set by users, which can be flexibly adjusted as a user-tailored type.

6. Conclusion

Network firewalls need to show robust performance because these are deployed in the front-end of trust network. In this paper, we experiment two firewalls operated by KIST. We can see that the SniperFW firewall provides 5~6 times improved bandwidth (throughput) to end-point server using ftp or GNU wget. At present, the KISTI is operating the SniperFW network firewall. However, whether duplicate or unused rules occur should be monitored continuously through log and rule analysis, and the access/deny rules of firewalls should be continuously managed according to the procedure that uses the naming convention. In addition, whereas the operating firewalls can provide services with further improved bandwidth to end-point users, users can affect each other if a quota per user is not specified. Therefore, it is necessary to establish a separate rule for specifying quotas and prepare a procedure through which users can apply and use quotas according to their needs.

7. References

1. Ahn BY, Jang JH, Ahn SI, Kim MI, On NR, Hong JH, Lee S. Study of high performance computing activation strategy. International Journal of Multimedia and Ubiquitous Engineering. 2014; 9(6):59–66.
2. Park CY, Yoon JW, Hong T-Y, Woo J. Pattern analysis of jobs on supercomputer TACHYON 2. Journal of Supercomputing Information. 2014; 2(1):15–9.
3. Hayajeh T, Mohd BJ, Itradat A, Quttoum AN. Performance and information security evaluation with firewalls. International Journal of Security and its Applications. 2013; 7(6):355–72.
4. Sheth C, Thakker R. Performance evaluation and comparative analysis of network firewalls. Proc IEEE Int'l Conf on Devices and Communications (ICDeCom); Mesra. 2011 Feb 24-25. p. 1–5.
5. Sheth C, Thakker R. Performance evaluation and comparison of network firewalls under DDoS attack. IJ Computer Network and Information Security. 2013; 5(12):60–7.
6. El-Atawy A, Samak T, Al-Shaer E, Li H. Using online traffic statistical matching for optimizing packet filtering performance. Proc of IEEE INFOCOM; 2007. p. 866–74.
7. Gouda MG, Liu AX. Structured firewall design. Computer Networks. 51(4):1106–20.
8. Liu AX, MG. Diverse firewall design. IEEE Transactions on Parallel and Distributed Systems. 2008; 19(9):1237–51.
9. Misherghi G, Yuan L, Su Z, Chuar C-N, Chen H. A general framwork for benchmarking firewall optimization techniques. IEEE Transactions on Network and Service Management. 2008; 5(4):227–38.
10. Funke, Reiner, Grote A, Heiss H-U. Performance evaluation of firewalls in gigabit-networks. Proc of the Symposium on Performance Evaluation of Computer and Telecommunication Systems; 1999.
11. Hayajneh T, Mohd BJ, Itradat A, Quttoum AN. Performance and information security evaluation with firewalls. International Journal of Security and its Applications. 2013; 7(6):355–72.
12. CISCO. Available from: http://www.cisco.com
13. WINS. Available from: https://www.wins21.co.kr
14. Iperf. Available from: https://iperf.fr
15. GNU wget. Available from: https://www.gnu.org/software/wget
16. Newman D. Benchmarking terminology for firewall performance. IETF RFC 2647; 1999.
17. Gouda MG, Liu ZX. Firewall design: Consistency, completeness and compactness. Proc International Conference Distributed computing Systems; 2004. p. 320–7.
18. Hamed H, El-Atawy A, Al-Shaer E. On dynamic optimization of packet matching in high speed firewalls. IEEE Journal on Selected Areas in Communiations. 2006; 24(10):1817–30.