DE GRUYTER
OPEN

JACSM 2017, Vol. 9, No. 1, pp. 49 - 63
10.1515/jacsm-2017-0003

Analysis of Performance and Efficiency of Hardware and Software Firewalls

Wojciech Konikiewicz[1], Marcin Markowski[2]

[1] Wroclaw University of Science and Technology,
Wybrzeze Wyspianskiego 27, 50-370 Wroclaw, Poland
wojciech.konikiewicz@onet.pl

[2] Department of Systems and Computer Networks,
Wroclaw University of Science and Technology,
Wybrzeze Wyspianskiego 27, 50-370 Wroclaw, Poland
marcin.markowski@pwr.edu.pl

Abstract

Firewalls are key elements of network security infrastructure. They should guarantee the proper level of security and, at the same time, the satisfying performance in order to not increase the packet delay in the network. In the paper, we present the comparative study on performance and security of a few firewall technologies including hardware, software and virtual solutions. Three important criteria are considered: the maximal throughput of firewall, the introduced delay and the ability to resist Denial of Service attacks. We report results of experiments, present analysis and formulate a few practical conclusions.

Key words: firewall, virtual firewall, network security, network performance, DoS attacks

1 Introduction

The security of telecommunication networks is one of the most important aspects of scientific research. When information is transmitted between users and servers, it often becomes the object of desire for unauthorized persons - the hackers, attempting to steal sensitive user data. Information security is especially important when the number of devices and end systems increases. IPS, IDS, anti-virus programs and, finally, firewalls are often placed on the border between the private and public networks. Choosing the proper security device is very important because it affects all the traffic passing between the local and external network.

Nowadays, firewalls are a mandatory part of the computer network in businesses, offices and other institutions. With the advancement of technology, these devices are constantly being developed. Their operation must be effective, quick and not noticeable to the potential users. There are many solutions available to protect the IT system. Some manufacturers provide their solutions for free, such as the programmable firewalls on Linux platforms, but there are also very expensive devices such as Cisco or Juniper hardware firewalls.

This paper focuses on selection of the best type of firewall for particular application. Optimal firewall should introduce the smallest packet latency in the network and, at the same time, provide a good protection level for user data. The goal of this work is to perform a comparative analysis of three types of firewall: two hardware solutions (Cisco ASA and Juniper), software solution installed on Linux (IPTables) and the virtual one(VyOS), implemented on a virtual machine. An analysis of the impact of individual firewalls on packet traffic in the network is based on bandwidth and server response time. We also analyze the level of resistance against the network attacks.

2 Firewall technologies

Firewall is a network device usually located at the border between two different (e.g. internal and external) computer networks. This is usually the place where the internal communication network of an enterprise is connected with the Internet. Its main task is to protect the network and data processed inside LAN. The firewall filters incoming and outgoing traffic. Thanks to certain rules, it is able to eliminate the unwanted traffic generated, for example, by an attacker. Firewalls control communication by deciding which packet is consistent with the security policy. Firewalls also isolate the restricted areas from the rest of the network. Firewall technologies can be divided into four basic groups: packet filtering, state control, network address translation (NAT), and proxy [2]:

- In *packed filtering* mode, device filters all incoming and outgoing packets, looking into the header information, i.e. IP addresses and port numbers. With defined Access Control List (ACL), only packets that are reflected in the security policy are allowed. It is important to start configuring the ACL with general (default) blocking rule, and after that to define which kind of traffic should be accepted. Filtering rules are usually defined separately for incoming and outgoing traffic [11].
- *Statefull firewall* is a powerful packet filtering technology, with control of the particular connection attributes. Unlike the packet filtering, it allows to monitor the connection status: whether the connection is in the

initiation, during data transfer, or in the termination state. Firewall tracks all the passing TCP sessions and drops packets, whose do not match any of known connections. Typically, the TCP rule is used for matching. This feature introduces a very high level of security, and it also offers satisfying transmission speed [14].

- *Network Address Translation* converts IP source (inside LAN) addresses into other (outside) addresses. This mechanism works on both sides, i.e. both outgoing and incoming packets are subject to this operation. This service does not have any built-in security services, but it allows to hide the internal architecture. Outbound packets live the local network with another IP address, so that the person or the external traffic tracking device is not able to see the local area network infrastructure [13].
- *Proxy Firewall* - this is a software package that gives an indirect access to the Internet. Communication on the network with the proxy server is split into two sessions: session between client and proxy service and session between proxy and remote destination server [14]. Client cannot connect directly to any server located in an external network.
- *Hybrid Firewall* is a combination of the above types of firewalls. In most applications it offers simultaneous packet filtering, the proxy services and allows to monitor the network traffic.

While the structure of the network is growing, the security devices evolve. At the turn of several years, three main types of firewall architecture (Figure 1) were created [11]:

- Hardware - a physical device that has its own resources: CPU, RAM, disk space. Similar to the router, having its own operating system.
- Software - a platform implemented on an existing operating system, using the resources of the server on which the OS is installed.
- Virtual - implemented as a virtual machine, most commonly used for packet filtering in SDN (Software Defined Networks) and for data protection in the cloud services. Thanks to the virtualization layer it is possible to change the hardware resources assigned to the machine [12].

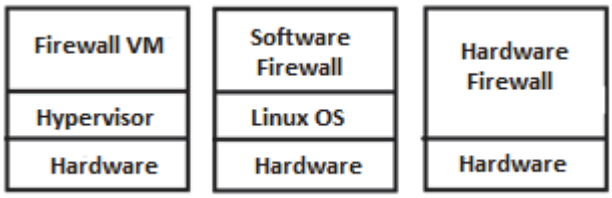

Figure 1. Comparison of firewall architectures

The hardware firewall is a stand-alone network device. It has dedicated components and the resources that it possesses are optimally tailored for correct and rapid work. Selecting a specific model of a hardware firewall, the manufacturers technical documentation should be carefully analyzed. An important feature of the hardware firewalls is that they are not dependent on third-part software. A software firewall is typically represented by a server with two network interfaces and a special application that is responsible for such functions as packet filtering, NAT or proxy. It controls the network traffic using configured bridge mode interfaces. All packets passing from the one subnet to the other are filtered according to the rules written by the administrator. Software firewalls do not have their dedicated resources. They use the resources of the operating system on which they are installed and cannot operate automatically. Software firewalls are very flexible, they can be extended with additional modules for proper operation, although their configuration is much more difficult since the majority of programs have only a textual interface. The advantage of the software firewall is that many free versions are available in the Internet. Virtual machines are running an environment monitored by the hypervisor. When multiple machines are running within a single virtual environment, a virtual network including all the physical network elements (routers, switches, and firewalls) is created [1]. Virtual firewall is responsible for the security of virtual host communication, but also for communication between the physical and virtual networks. Some virtual firewalls integrate additional network features such as VPN or QoS. Virtual firewalls do not have dedicated hardware resources but use the resources provided by the virtualization layer. The advantage of such solutions is the flexibility to change the hardware parameters of each machine.

3 Related Works

While surveying the scientific papers, we will not find an article or book comparing all types of firewalls. The main topics of the research are the optimization of device operation and the virtualization of particular elements of the backbone network. In [1] Author describes the use of the virtual gates and shows the basic differences between traditional and software firewalls. The advantages of non-physical applications, as well as the disadvantages of these technologies, are analyzed. The article does not present any exhaustive comparison, it just proposes the area of application of considered gate. Also the structure of the virtual network in which this device could be implemented have been proposed. In [2] Authors compare a few types of firewall technologies: packet filtering, statefull firewall, proxy, and hybrid firewall. The article does not contain any simulation data and therefore does not indicate the best system. Authors focused on the description on how the

firewall works and what its advantages are. The second part of the article deals with the subject of intrusion detection and prevention systems. The summary of the article is a table with the advantages and disadvantages of considered technologies.

Comparison of hardware and software firewall may be found in [3]. Cisco ASA 5500 (hardware), Check Point SPLAT (software) and Open BSD PF (software) were verified against the simulated DDoS (*Distributed Denial of Service*) attacks. Authors have shown that none of the firewalls are immune to this kind of threat. The results presented in the publication have been based on laboratory simulations and summarized in the table. According to the tests, all the firewalls showed similar performance, but SPLAT was the best one, able to survive 15 minutes attack. Another important parameter measured during this simulation was the CPU consumption level, best results were obtained for Cisco ASA. Devices listed in the above article are also the subject of research in papers [9] and [10]. Authors present a simulation-based comparison on the HTTP, FTP, UDP packet throughput and the number of possible connections. In [9] the security level of devices was also compared and some considerations on the degree of complexity of configuration, important when choosing a device by less experienced administrators, were presented. As the results have shown, both Cisco ASA and Check Point are doing very well with packet filtering, but Cisco hardware is the best one when taking into account the offered bandwidth. Paper [4] deals with the topic of firewalls, from definition to simulation. The study focuses on comparing commercial and free software firewalls. It includes both platforms configured under Unix operating systems (Linux, BSD, Solaris) and Windows (WS 2003). That work is based on an extensive simulation part, which is summarized by the graphs showing the packet delay dependence on the number of connections and the size of the packets. Summary of publications is a presentation of the disadvantages and advantages of each platform. The main advantage of the article is the well written theoretical part. The other articles discussing the subject of firewall comparison are [5] and [6]. Both compare hardware firewalls with software ones, but in [5] the considerations are purely theoretical. Author of [6] have investigated Cisco hardware firewall and platforms implemented on Linux. The comparison is based only on the data provided by the manufacturer and security tests made with basic security tools such as *nmap*. Very similar topic, a comparison of a firewall implemented on the Linux platform and the Cisco 2621 firewall, is addressed in [8]. That study shows the number of TCP packets passing through a device per unit of time. Definitely better results were obtained for Linux which, for the number of filtration principles 0-200, achieved two times higher bandwidth. Article [7] contains a comparison of the firewalls built into operating systems. Authors have generated identical traffic directed to two servers (Windows and Linux)

and investigated the CPU utilization. The results show that firewalls significantly affect the load of the platform on which they are implemented.

There are many works, publications and articles describing firewalls, but there is a restricted number of comparisons between all types of devices. Usually the hardware and software firewall comparison may be found. Since virtual firewalls are not yet very common then, in the literature, the architecture of the virtual systems is often considered. Comparisons mostly refer to Cisco devices as the leading physical ones, OpenBSD and Check Point as a software firewalls.

In this work we examine three types of firewalls: hardware, software, and virtual. We provide the comparative analysis and conclude, which of solutions ensure the best performance and the minimal impact on the network traffic.

4 Problem formulation and experimental setup

A network topology built of two computers and a traffic filter device (hardware firewall or dual-homed server with software/virtual firewall) was implemented for the experiments (Figure 2). One of the computers (SERVER) served as a server and was placed behind the firewall internal interface, the second one (PC) was placed in an external network zone. All analyzed firewalls were configured in the similar way in order to make the result comparable. The whole infrastructure was connected using category 5e UTP twisted pair copper cable.

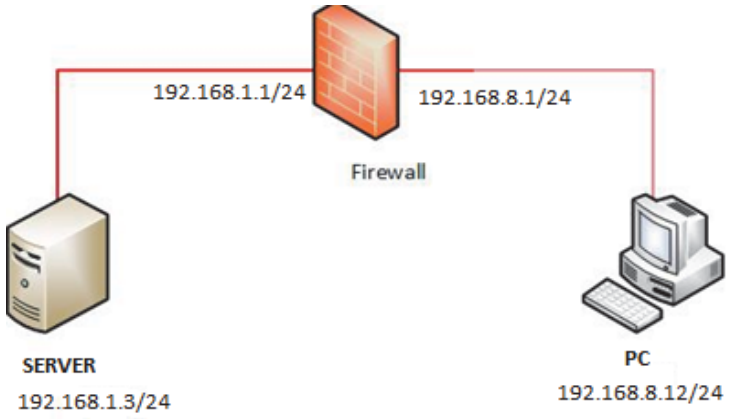

Figure 2. The network topology

Four firewalls were analyzed: IPTables, (software firewall), Juniper Netscreen 50 and Cisco ASA 5505 (hardware) and VyOS (virtual firewall). IPTables is a free software that is installed on the Linux operating system. It

has the ability to work from the second to the seventh ISO/OSI layer, then it can work as a comprehensive firewall. With the open license it is constantly being expanded with additional functionalities and support for additional protocols. The basic feature of IPTables used in this study is the packet filtering. It is based on the rules in the strings (equivalent of access-list), which are placed in the tables. The rules are the most important elements in the firewall configuration, because they determine whether the packet is accepted (ACCEPT) or rejected (DROP) [7].

The Juniper Netscreen 50 is a firewall with four Ethernet ports with a maximum throughput of 100 Mbps. The device supports two operating modes: transparent firewall and router with built-in firewall. In the former one, device acts as a second layer bridge and is invisible to other devices in the network. It filters packets according to established rules, but it has NAT disabled, because it cannot interfere with packet addressing as a second layer device. In the latter mode the firewall operates in the third layer and requires configuring the IP addresses of the individual interfaces. This allows NAT to be started [15]. An additional feature of Netscreen 50 is the ability to run the VPN functionality.

Cisco ASA 5505 has eight 10/100 Mbps network ports, two of them with a Power over Ethernet (PoE) functionality. Network interfaces of the firewall work in Layer 2 only, then it is impossible to configure IP addresses directly on the interfaces – they must be assigned to the appropriate virtual interfaces (VLANs). It is possible to assign each interface to another VLAN and isolate the subnets. VLANs can communicate with each other directly through the firewall, where packet filtering is applied. Devices on the same subnet exchange packets bypassing filtering. In order to divide the network into trusted and non-trusted interfaces, the security levels are defined and labeled from 0 to 100. The higher number, the higher security level. It is important that higher levels may access the lower-level interfaces, but not vice versa [16].

VyOS is a virtual platform with router and firewall functionalities, created in 2013 as a free network operating system. It is based on Debian and Quagga platform. VyOS configuration is provided through the CLI interface. It can be installed on virtual machines or on the cloud-based platforms. VyOS has been equipped with all the features of a physical firewall: packet filter, NAT service, VPN, and routing mechanisms. It is suitable for large and small networks as an alternative to physical devices, what remarkably reduce costs [17].

The common network diagnostic tools: *iperf*, *ping* and *hping* were used for the experiments. *Iperf* is a free network tool for measuring network bandwidth. It supports various protocols including: TCP and UDP. Thanks to the large number of parameters, it is very useful. For each performed test, it generates a report containing the connection throughput in the subsequent

time units [19]. *Ping* is a popular program used by the computer network administrators to diagnose the network performance, it is based on ICMP protocol. It allows to verify the connection between hosts, and measure the number of lost packets [18]. *Hping* is a tool for networks and devices analyzing. It can serve as a package generator and is often used for network audits. It supports protocols such as TCP and UDP. Additionally, it has features for sending files and the ability of package route tracking. *Hping* was originally created as a tool for the network testers, but is currently used by hackers as well [20], as able to carry out the *DoS* attacks (this option was used during experiments).

5 Experiments and Results

The goal of experiments was to obtain an comparative analysis of firewall solutions on their performance, efficiency and resistance to Denial of Service attacks. Considered criteria taken into account were: the throughput of firewall (in Mb/s), delay introduced by firewall and time of surviving during DoS attack.

For throughput investigations, *Iperf* tool was used to generate a high intensity traffic from PC to Server. In the consecutive experiments, different packed sizes l (in Bytes) were used, the intensity (in Mb/s) of generated traffic was always the same, equal to maximal possible line speed (around 100 Mb/s). The higher value of l, the smaller number of packets was sent during one second. As a baseline we have also measured a throughput in the direct connection between PC and Server (without firewall). Each single experiment lasted 60 seconds. Experiment with each packet size were performed a few times and results for each second were averaged. They are presented in Figures 3-6. It may be observed that the throughput of firewalls is unstable for l=200B and l=500B (Figure 3 and Figure 4). For l=200B the measured throughput was between 20 Mbps (for virtual firewall VyOs) and 80 Mbps. For l=500B (Figure 4) the significantly higher throughput was observed for VyOS (around 45 Mb/s), slighter improvement was noticed for the other firewalls, as well as for direct connection. Comparing results for both packet sizes it may be concluded, that the number of packets processed during one second is much about the same in case of VyOS – the higher number of packets, the higher throughput (in Mb/s).

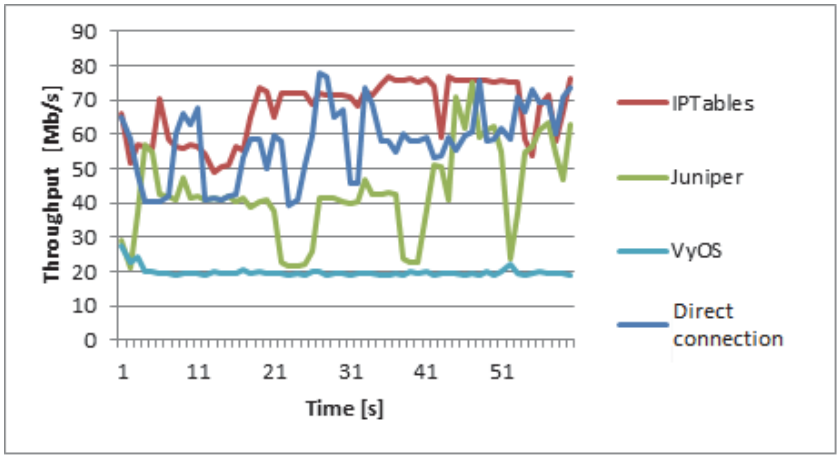

Figure 3. Comparison of the throughput for *l*=200B

Unexpectedly, the throughput offered by PC-based firewall (IPTables) was often higher than offered by dedicated network device (Juniper). The above observation is very interesting, since hardware firewalls are considered as offering much better performance in comparison with the multi-purpose computers. Also the throughput for the direct connection is very uneven, for *l*=200 the throughput of IPTables seems to be higher than throughput of direct connection. We may conclude, that for small packet size (and high number of packets per second) the performance of the PC network card or properties of TCP protocol (devices receives new packets and, at the same time, have to send acknowledgments of received packets) may hardly affect the results.

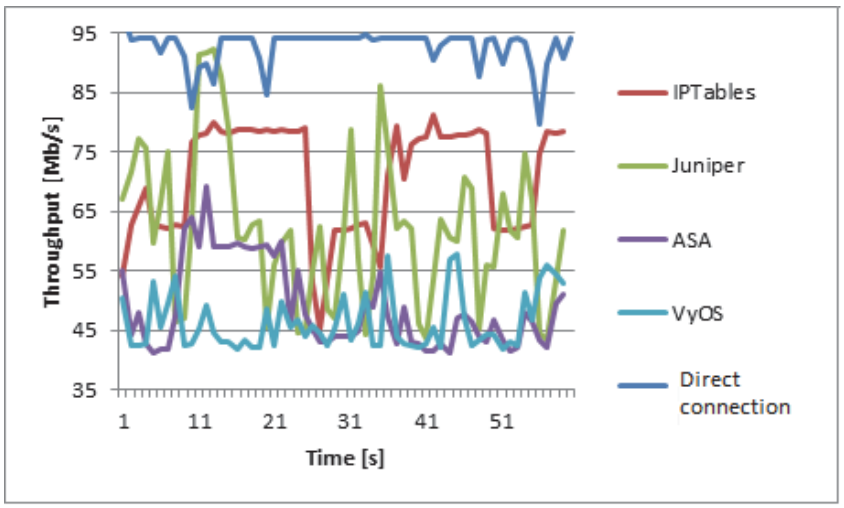

Figure 4. Comparison of the throughput for *l*=500B

Analyzing results for bigger packet sizes (Figure 5 and Figure 6), it can be observed that the throughput for ASA and IPTables are very close to the real bandwidth of the direct connection between computers. Those firewalls do not introduce any decrease in the network performance. A little bit worse and less stable results were obtained for Juniper. The lowest performance was noticed for the virtual firewall, where the value of throughput oscillated between 65 and 80 Mbps. For l=1500B, throughput of hardware firewall tends to be unstable. Comparing results presented in the Figures 5 and 6 we may conclude, that packet size equal to 1 kB was optimal in prepared testbed environment.

Average (taking into account values from each second of each experiment) values of throughput for all firewalls and sizes of packet are presented in the Figure 7. Improvement in the firewall performance with the growing size of

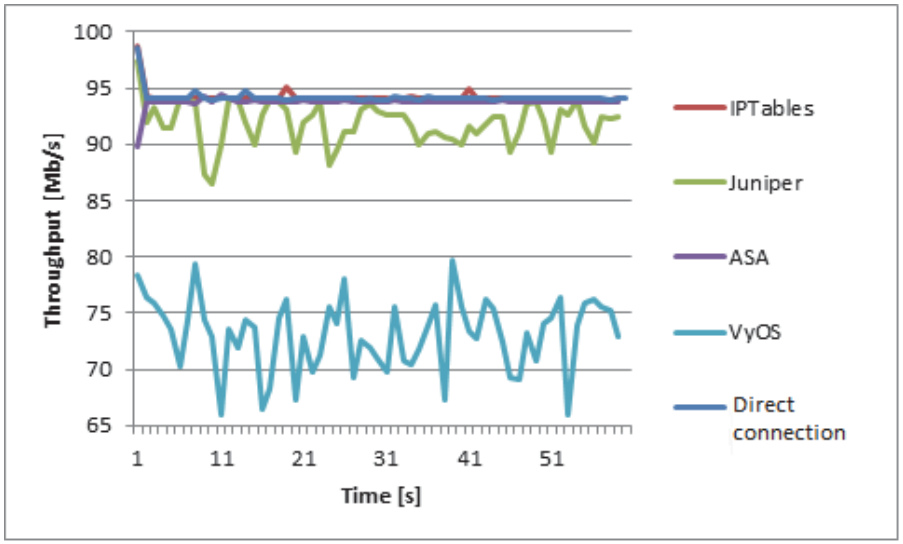

Figure 5. Comparison of the throughput for l=1000B

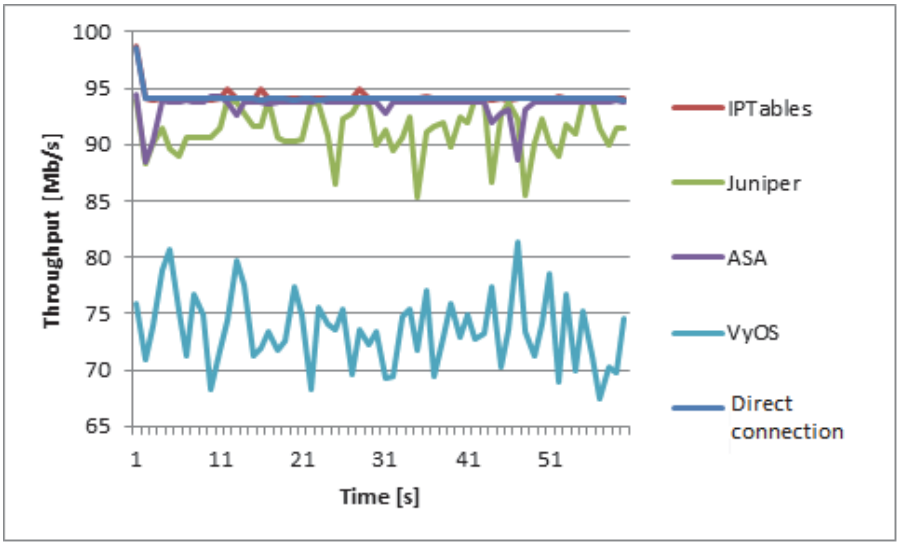

Figure 6. Comparison of the throughput for *l*=1500B

packet may be clearly seen. For *l*=200B all firewalls offered the least performance, but with the increase of the packet length the performance increased. For *l*=1000 and *l*=1500 the throughput reached a maximum value equal to the direct connection one. The graph shows that the slowest firewall turned out to be a virtual firewall, and hardware and software ones achieved very similar results.

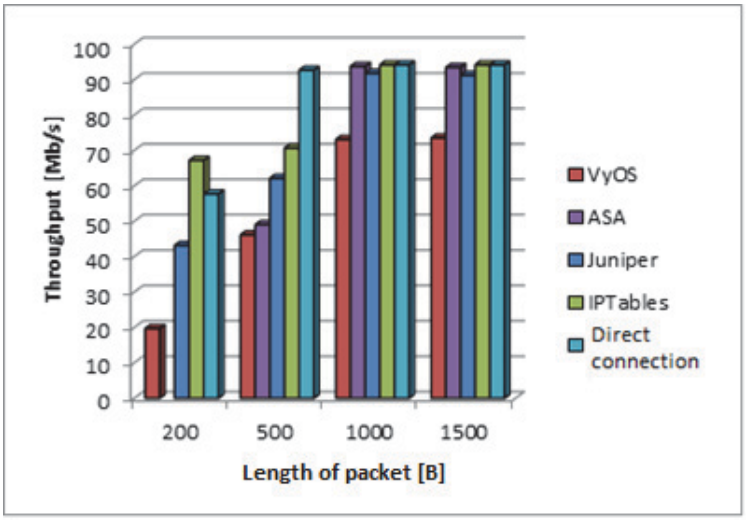

Figure 7. Average throughput for all firewalls

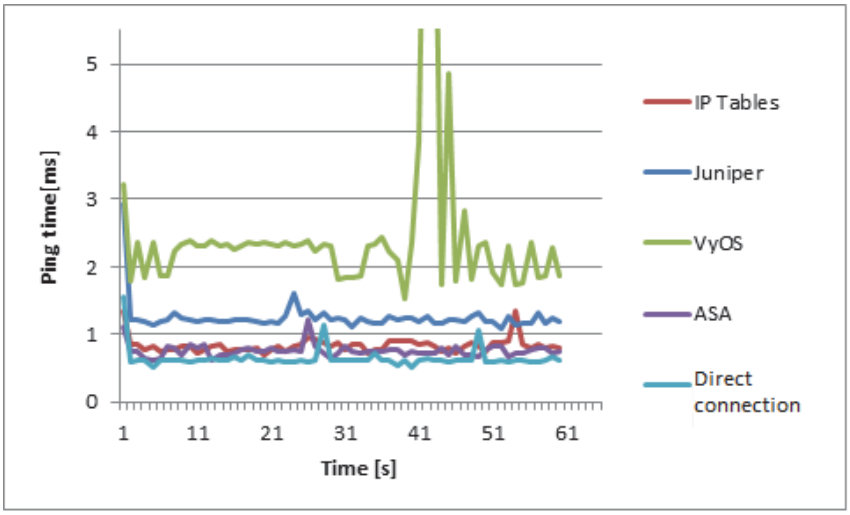

Figure 8. Ping response time for packet size 64B

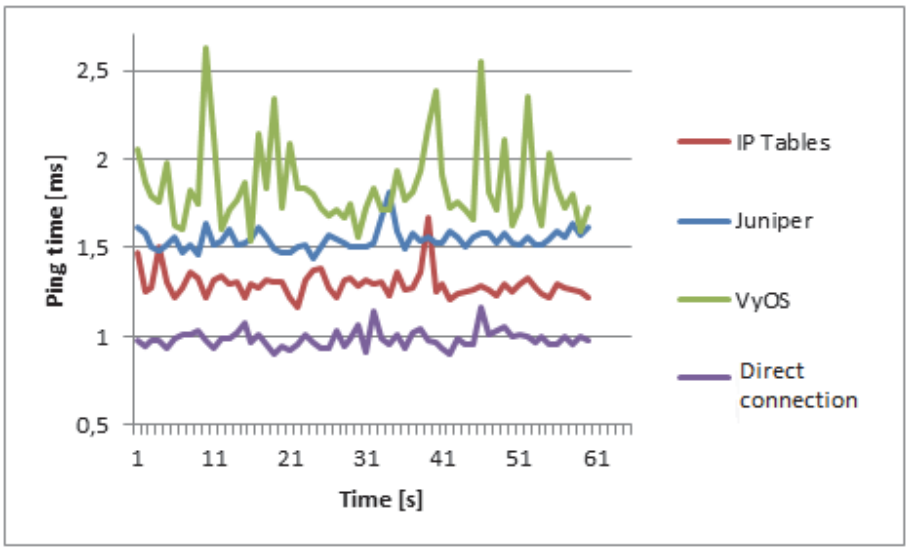

Figure 9. Ping response time for packet size 1000B

During the second part of the study the server response time was examined. The research was done using a *ping* program showing the time the packet reaches its destination. Results of these studies show which firewall introduces the greatest latency in the network. Experiment were performed in the following way. Each device was examined twice, with two packet sizes: 64 B and 1000 B. Each experiment (with each packed size) last for 60 seconds. As it may be observed in the results (Figures 8 and 9), the highest delay was observed for VyOS. Delay introduced by virtual firewall definitely

differs from the others. The smallest delays were observed for ASA and IPTables. The average response time for packet size equal to 64B was at the level of 1ms (for ASA, Juniper, IPTables) and 2.5ms for VyOS. In the latter study (ping size 1000B) the response time increased to 1.25ms for Juniper and IPTables, but we have observed a little decrease in the delay introduced by VyOS. Result for all examined firewall became proportionate.

Comparing results for all experiments it is clearly seen that virtual firewall may be pointed out as the worst solution, taking into account the performance and efficiency. It may be due to the fact that the virtual machine does not have its own built-in interfaces but uses communication interfaces of the physical machine on which it is installed. Transmitting packet through each physical port is there an additional delay. The virtual firewall could achieve better results when tested in the virtual network, which is its dedicated environment.

Finally, the ability to survive the Denial of Service attack was examined for all firewalls. DoS attack was carried out for 30 minutes with *hping3* tool. At the same time the availability of network connection to firewall was verified using *ping* requests. VyOS, ASA and Juniper remained available and operational during attacks. The CPU utilization around 100% was observed for each of them, but *ping* responses were received all the time during experiments. Unlike the others, IPTables stopped to response after 35 seconds, and hanged out after next 15 seconds. The restart of operating system and renewing of configuration was necessary in order to restore firewall functionality. It is worth to notice, that in case of software firewall the DoS attack was pointed at the operating system (Linux in this case), not at the firewall itself.

6 Conclusion

In the paper the performance and security of the hardware, software and virtual firewalls have been analyzed. The analysis was based on experiments in the prepared network environment. The considered criteria were: the throughput of the firewall, the introduced delay of network packets and the resistance to DoS attacks. A few important, practical conclusions were drawn from the results of experiments. It have been observed that the throughput of firewalls strongly depends on the size of packet transmitted over the network. Highest throughput, very close to the capacity of direct connection, was noticed for packets length equal and greater than 1 kB, for smaller packet lengths the throughput was considerably less. We may conclude that the optimal size of packet is 1 kB, while using network firewalls. Very interesting conclusion is the fact that the performance of the software based firewall was equal to the performance of hardware ones. In prepared physical environment the performance of virtual solution was lowest during all experiments.

Hardware and virtual firewalls turned out to be resistant to Denial of Service attacks. As documentation shows, they have built-in mechanisms for DoS protection. We became convinced that those mechanisms are effective. The level of security of the software firewall is, in fact, equal to the security level of the host operating system.

References

1. Ramaswamy Chandramouli, 2016, Secure Virtual Network Configuration for Virtual Machine (VM) Protection, NIST Special Publication 800-125B.
2. Wankhade A., Chatur P.N., 2014, Comparison of Firewall and Intrusion Detection System, International Journal of Computer Science and Information Technologies, Vol. 5 (1), pp. 674-678.
3. C. Sheth, R. Thakker, 2013, Performance Evaluation and Comparison of Network Firewalls under DDoS Attack, Computer Network and Information Security, Vol. 12, pp. 60-6.7
4. T. Höfler, C. Burkert and M. Telzer, 2004, "Comparative Firewall Study," Chemnitz Univeristy of Technology, Chemnitz.
5. Panchal R., 2005, *Firewalls: Hardware vs. Software*, SE 4C03.
6. Krajnik B., 2004, Firewalls with Filtering in Application Layer and Quality of Services, Engineer Diploma Thesis, Warsaw University of Technology.
7. Gouri Shankar Prajapati, Nilay Khare, 2015, A Comparative Study of Software Firewall on Windows and Linux Platform, International Journal of Computer and Technology, Vol. 14(8), pp. 5967-5978.
8. S. Patton, D. Doss and W. Yurcik, 2000, Open source versus commercial firewalls: functional comparison, Proceedings 25th Annual IEEE Conference on Local Computer Networks. LCN 2000, Tampa, FL, pp. 223-224.
9. C. Sheth and R. Thakker, 2011, Performance Evaluation and Comparative Analysis of Network Firewalls, 2011 International Conference on Devices and Communications (ICDeCom), Mesra, pp. 1-5.
10. Y. Yongxin, 2011, The comparative study on network firewalls performance, 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, pp. 427-430.
11. Shinder T.W., Shimonski R.J., Shinder D.L., 2003, The Best Damn Firewall Book Period" Syngress Publishing, Rockland.
12. Decusatis C., Mueller P., 2014, Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network, 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Systems (HPCC,CSS,ICESS), Paris, pp. 819-822.
13. Comer D.E., 2012, Computer networks and Internets, Helion, Gliwice.
14. Krysiak K., 2005,. Sieci komputerowe. Kompendium. Helion, Gliwice.

15. NetScreen Technologies Inc., Juniper Netscreen Instaler's Guide, Version 4.
16. Gałęzowski G., 2010, Cisco ASA 5505 Podstawy konfiguracji, HAKING, Vol. 12/2010.
17. wiki.vyos.net
18. linux.die.net
19. iperf.fr/
20. blackmoreops.com, Denial-of-service Attack – DoS using hping3 with spoofed IP in Kali Linux, 2015.