International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.355-372
http://dx.doi.org/10.14257/ijsia.2013.7.6.36

Performance and Information Security Evaluation with Firewalls

Thaier Hayajneh, Bassam J. Mohd , Awni Itradat, and Ahmad Nahar Quttoum
Computer Engineering Department, The Hashemite University, Zarqa, Jordan
Emails: Thaier@hu.edu.jo, Bassam@hu.edu.jo, itradat@hu.edu.jo, quttoum@hu.edu.jo

Abstract

Firewalls are an essential part of any information security system being the first defense line against security attacks. 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. In this paper, we present an assessment methodology to analyze the performance of different firewalls platforms. The analysis considers the following metrics: delay, jitter, throughput, and packet loss. Moreover, the information security of the firewalls is also tested by applying a set of attacks and observing the reaction of the firewalls. The proposed assessment methodology is tested by performing real experiments on different types of firewalls including those that are personal and network-based. Moreover, a quantitative study is conducted to explore the level of knowledge among the educated category in the community, represented by a sample of college students, on the importance of firewall and their use.

Keywords: *Firewalls evaluation, Firewalls attacks, network-based firewalls, Personal firewalls*

1: Introduction

The concept of having an institution or organization network as an isolated LAN is no longer applicable. Everyone wants to be online and have Internet access. This accessibility is intriguing to attackers with malicious intentions to breach the network and access its assets. Attempting to protect workstations individually is not practical. A better solution is to use a firewall to isolate the LAN from the Internet and examine all the traffic going in and out of the network.

The integration between intranet and the Internet requires a secure gatekeeper to protect against network-based security attacks. Firewalls usually protect the network from such threats while continuing to allow information exchange with the outside world. Hence, defining a firewall as a device providing a perimeter security is not a valid definition. Although system administrators work to enforce their network traffic to pass through the firewall, some internal users continue to have an Internet connection that bypasses the firewall.

A firewall must guarantee that only authorized users access an operating system or a computer connected to a network, securing by that private information and defending

ISSN: 1738-9976 IJSIA

computer users from identity theft. In most cases, firewalls block unauthorized access that computer users are not aware of.

Firewalls are categorized into two main types: network-based and personal [18]. A network-based firewall is usually installed at the edge of the network connecting the LAN with the broadband access. A personal firewall, also known as desktop or software firewall, is a program that is installed on personal devices (e.g., laptop) similar in that to an antivirus. In most cases, system administrators install both types of firewalls in order to protect against attacks that bypass network-based firewalls and to provide layered security.

Little work is done on assessing the impact of firewalls on network performance and their resilience against security attacks. Since a common concern of network users is the efficiency of the used firewalls, in this paper we present an assessment methodology to analyze the performance of different firewalls platforms. The performance analysis considers delay, jitter, throughput, and packet loss. The security of firewalls is also tested by applying a set of attacks and observing the reaction of the firewalls. The proposed methodology is tested by performing real experiments on different types of firewalls including those that are personal and network-based.

Moreover, computers became convenient in every household, company, educational institution, entertainment venue, and other public areas. Most of the users are non-professionals including students, employees, children, and other users. This means that most users have little knowledge on network security, if any. Therefore, a secondary objective of this paper is to explore the level of knowledge of a sample of college students on the importance of firewall and their usage. To study this issue and the aforementioned objective a quantitative study was conducted and the results and conclusions are illustrated in this paper.

The rest of this paper is organized as follows: Section 2 summarizes previous work conducted in this area. Section 3 provides a background on firewalls and their classification. Section 4, presents the firewall assessment methodology. Section 5 illustrates the system and hardware implantation. Section 6 presents the results of firewall performance evaluation. Section 7 describes firewall security evaluation results. A study of firewalls usage and awareness is illustrated in Section8. Finally, Section 9 concludes the paper.

2: Related Work

Little work was published on firewall performance analysis. Most of the available work considered enhancing firewalls configuration management and detecting misconfiguration as presented in [7, 19, 12, 11, 8].

Salah et al. [16] studied the performance of firewalls using analytical queuing model based on Markov chain. The methodology analyzes firewalls that are subject to normal traffic flows as well as DoS attack flows.

In [17] the researchers examined various types of firewalls operations. They tested the performance and security for various firewalls including: Cisco ASA, packet filter, and Checkpoint SPLAT. In terms of performance, the researchers only considered the throughput and the maximum number of concurrent connections. Their results showed that Cisco ASA provides better performance compared to the other two firewalls. As for security, they performed simple tests and reported that the firewalls demonstrated good resistance.

In [13] the researchers studied the effect of implementing a firewall on the network performance. Their simulation results showed that using firewalls increases the network delay

and average response time. Moreover, they suggested using parallel firewalls to improve the network performance. Researchers in [5] investigated the performance of application layer firewalls in terms of response time and link utilization. The simulation results proved that firewalls degrade the performance of the network.

In [6] the researchers experimentally evaluated and modeled Linux kernel firewalls focusing on the error-caused security vulnerabilities and resulting security violations. In [10] the researchers showed that using DNS rebinding can circumvent firewalls and disrupt an intranet. They proposed the use of a personal tool called dnswall to combat firewalls circumvent.

In summary, none of the previous work presented a comprehensive analysis on the impact of firewalls on the network performance. Therefore, this paper aimed to compare network-based and host-based firewalls in terms of performance and security.

3: Types of Firewalls

A firewall can be defined as an electronic device or program that manages the flow of data and information that are going in or out of a network. The aim is to prevent unauthorized access to the network from an adversary which could lead to data loss and exploitation of the services. In computer networks, firewalls are the gatekeeper of the network that examines all incoming and outgoing data packets to determine whether they are authorized or not based on a set of predefined rules.

The idea of firewalls is to construct a bridge between an internal private network or system(that is assumed to be secure and trusted), and the out side world (i.e., the Internet which is public, untrusted, and contain adversaries).

Firewalls are roughly classified into personal and network based firewalls [18]. Personal or also called "host-based" firewalls are usually software applications that are installed to run on the operating system. Nowadays, most of the operating systems come with a built-in firewalls. Personal firewalls are becoming very popular and they aim to protect individual hosts from malicious packets by performing host packet filtering. While network-based firewalls are available, one would question the need of personal firewalls. Moreover, personal firewalls are the best, if not the only, option for mobile users. In addition, they protect against connections that bypass the network firewall to form a layered defense. In personal computers, firewalls test whether an installed software is allowed to access the Internet, performing by that what is known as egress filtering.

Network-based firewalls consist of: hardware, software, and firmware that are particularly optimized for firewall functionality. This makes them capable of providing a higher performance compared to personal firewalls. Other advantages include:

- Simplifying security management
- Facilitating implementation of advanced logging and monitoring
- Allowing creation of a VPN using IPSec to other hosts
- Enabling segmentation and isolation of problems
- Hiding the IP addresses of client stations in an internal network by presenting one IP address to the outside world

On the other hand, disadvantages of network based firewalls include being a bottleneck and a possible single point of failure. This strictly requires firewalls to be as tamper proof

as possible and to operate with high efficiency to avoid degrading the network performance. Figure 1 shows the main types of firewalls [18].

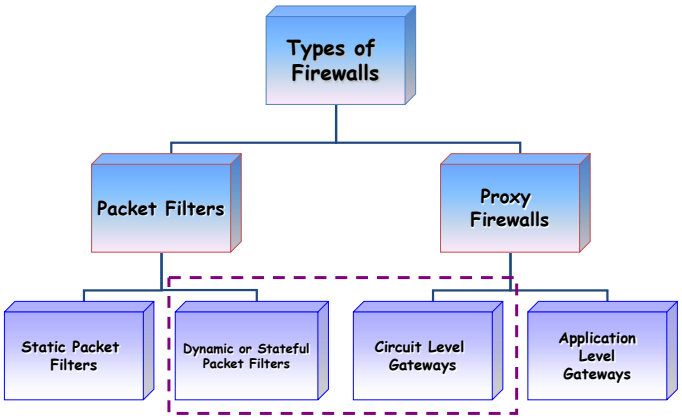

Figure 1. Types of Firewalls

Packet filtering firewalls are the simplest firewalls which is mostly a router that has capability to filter packets . They typically work on layer three and layer four of the OSI model. Packet filtering rules are defined to match the packets and determine which traffic is allowed or denied . The main advantage of packet filtering firewalls is their simplicity and capability to quickly process packets in order to provide protection against attacks. Despite the advantages of packet filters they cannot prevent application layer attacks and are susceptible to certain types of TCP/IP protocol attacks.

Stateful firewalls are more intelligent than packet filters as they examine the state of a connection when data being initiated, transferred or terminated. A stateful firewall examine information in the packet header of layer 3 and layer 4. For example, it looks at the TCP header for SYN, RST, ACK, FIN to determine the state of the connection.

The stateful firewalls can detect the state of the connection and can prevent some types of DOS attacks. Generally, stateful firewalls are used as an intelligent first line of defense without adding extra cost. However, they cannot prevent application layer attacks and may cost an additional overhead in maintaining a state table.

Proxies firewalls, unlike other firewalls, they reproduce application layer functionality where packets are not examined individually but rather collectively decoded instead. Examination after decoding usually indicates whether or not the packets belong to a valid request. Proxy firewalls, also known as gateways, act as a relay for applications. The users in a LAN contacts the proxy with identification information. Then, the proxy acts on the behalf of the user and contacts the application server. Afterwards, it relays packets between the user and the application server while shielding either side from direct connection.

The proxy needs to be configured for each service (e.g. e-mail, web, FTP) the administrator wants to provide in the network. Proxies provide a deeper traffic examination and consequently deliver higher levels of security. However, this advanced level of security compromises the network performance network in terms of delay, jitter, and throughput. Another drawback of using a proxy is that disturbing it causes the entire network to malfunction. Attackers are usually aware of this vulnerability which makes proxies an obvious target.

4: Evaluation of Firewalls

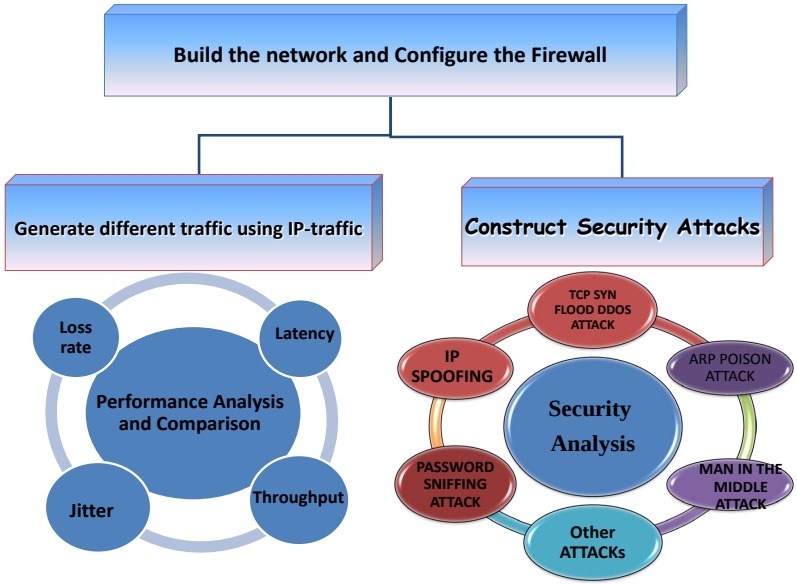

Figure 2. Assessment methodology

In this paper, we propose an assessment methodology for evaluating different types of firewalls in terms of both performance and security. It is always desired to have secure and attack-resilient firewalls, however, performance degradation could be a concern. With the evolution of today's Internet and the extensive use of multimedia application by the users, network QoS becomes a priority for the users. Figure 2 shows the assessment methodology for evaluating a firewall. At first, the firewall QoS performance is tested under different traffic scenarios. Then, the security of the firewall is evaluated under several attacks.

4.1: Performance Evaluation Criteria

The performance of a firewall is usually tested under different traffic loads while considering several metrics to evaluate the firewall performance. In this paper, we focus on the following metrics:

- Throughput: is the actual payload that is received per unit of time [14].
- Delay: is the time it takes a packet to be transferred from the source to the destination.
- Jitter: measures the variation in delay of the received packets.
- Packet-loss-rate (PLR): is the ratio of the lost packets to the total transmitted packets.

4.2: Security Analysis

Unlike QoS evaluation, security is not an absolute quantity and no quantitative approach exists to evaluate it. Hence, in this paper we built a testing methodology to evaluate the security performance of different firewalls. The testbed consists of two computers and a firewall, where one computer represents the victim and is supposed to be protected by

the firewall. The other computer represents the attacker which will be generating attacks through the firewall. If the attacking computer successfully managed to read any data, scan the opened ports, or make the victim computer busy or unable to perform other tasks (DoS attack), the attack is considered successful and the firewall would fail the test. Otherwise, if the attacker completely failed to do any of the above- mentioned problems, then the firewall would have been considered to succeed the test. Finally, if the attacker partially succeed then the firewall partially fail the test. The details of the attacks and their deployment tools are discussed later in Section 7

5: Testing and Hardware Implementation

In this section, we describe the testbench used to conduct the experiment, the hardware devices and the software tools used to collect and analyze the results. We also present the experimental scenarios conducted for studying the impact of firewalls on several network performance metrics such as throughput, delay, jitter, and packet loss ratio. Clock synchronization will also be discussed in this section. Finally, traffic streams used in this experiment will be illustrated.

5.1: Testbench and hardware Description

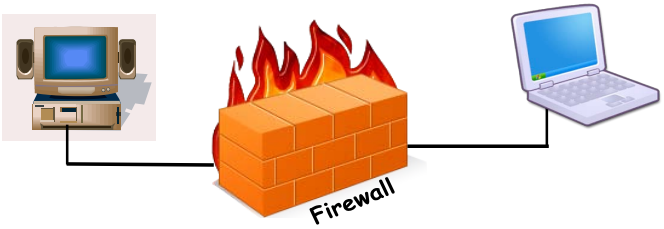

Figure 3. Experimental Testbench

The testbed used for the experimental testing is shown in Figure 3 which shows two computers connected through a firewall. The two computers were notebooks with the following specifications:

- CPU: Intel core i5, 2.24 GHz processor.
- NIC model: Realtek RTL Gigabit Family.
- Operating system: Ubuntu 11.04 and Windows7

Two network-based firewalls were used in the experiments: Cisco ASA and packet filter (PF) firewalls. The Cisco ASA 5510 is an adaptive security appliance that provides high-performance firewall and VPN services[2]. It is usually suitable for small and medium-sized businesses and enterprise remote branch offices as an easy-to-deploy, cost-effective appliance. As for the packet filter, we used the Cisco 2811 router with extended ACLs. Table 1 shows the specification of the two network-based firewalls that are used in the experimental testing. Although the implemented testbed setting is simple with one computer to generate the traffic, however, the generated traffic mimics the traffic that may be generated from a complex network that exists in large organizations.

Table 1. Network based Firewalls' Specifications

Feature	ASA	PF
Model	Cisco ASA 5510	Cisco Router 2811
Operating System	IOS V8.3(1)	IOS V 12.4(3)
Memory	1 GB	256 MB
Processing Speed	1600 MHz	350 MHz
Interfaces	5 Fast Eth. ports; 2 Gigabit Eth.	2 Fast Eth.
Connections/ Second	9000	NA
Firewall Throughput	Up to 300 Mbps	NA
Concurrent Sessions	50,000-130,000	NA

5.2: Clock Synchronization

Accurate synchronization for the Laptops clocks is crucial to avoid erroneous results on delay and jitter. To ensure precise clock synchronization, we used the AtomTime Pro software [1], which frequently connects to global servers to adjust the time of the devices used in the experiment. As for the communication with the time server, an out-of-band connection was used to guarantee no interference with our traffic.

5.3: Traffic Streams

The test traffic is generated using IP traffic generator tool [4]. IP traffic is a data generation tool for IP networks that can generate TCP and UDP traffic at different rates. The firewalls are tested under different loads: light, medium, and heavy loads. The traffic consists of 16 concurrent connections with 500, 10000, 30000 packets generated for each connection for the light, medium, and heavy loads, respectively. Two different packet sizes are considered: 1460 and 512 bytes.

6: Performance Evaluation Results

In this section, results from both scenarios are discussed in terms of delay, jitter, and throughput. For statistical validation, all the experiments were repeated 10 times and the averages were considered in our results.

6.1: Network Based Firewalls

Figure 4 shows the throughput in Mbps with TCP traffic for ASA and packet filter firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. For the same load and packet size, the figure shows that ASA firewall has significantly higher throughput compared with packet filter. As discussed earlier, this result is expected due to the fact that ASA consist of specialized hardware and software. For all cases, increasing the traffic load obviously increases the throughput. Moreover, packets with 1460 results in higher throughput. The results from throughput confirms that ASA is suitable for large networks with high traffic rates.

Figure 5 shows the throughput in Mbps with UDP traffic for ASA and packet filter firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. As

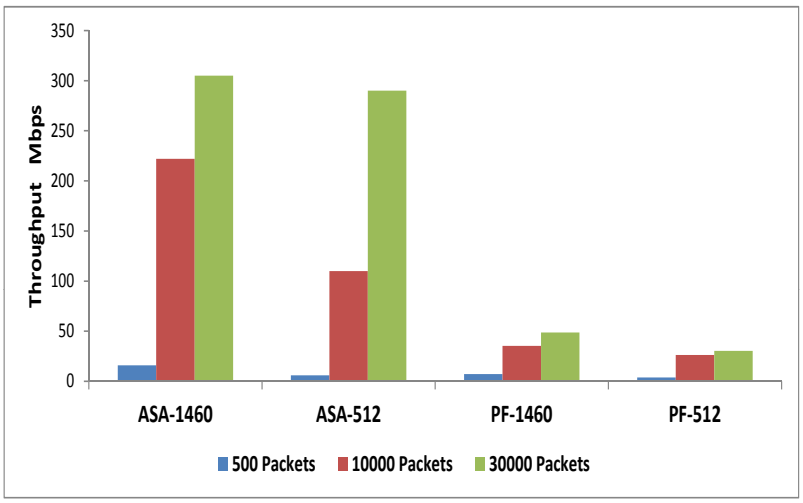

Figure 4. Throughput of Network Firewalls with TCP

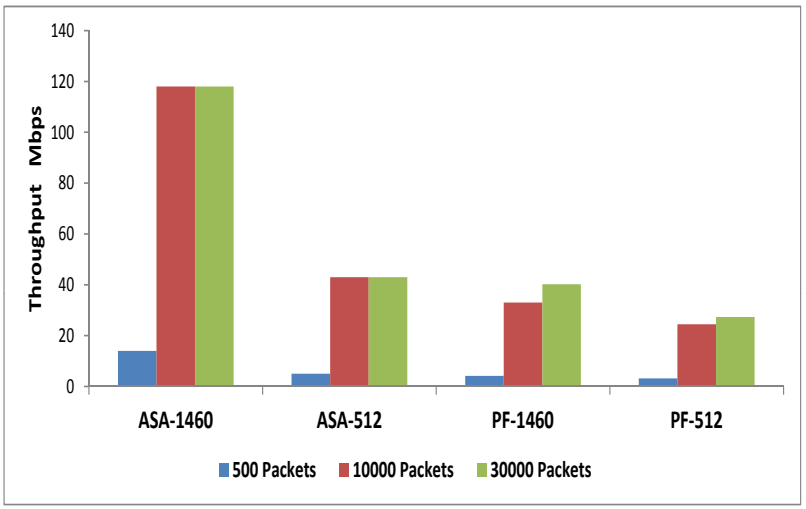

Figure 5. Throughput of Network Firewalls with UDP

shown in the figure, with UDP traffic, the firewalls reached a lower throughput. Figure 5 also shows that with UDP traffic the firewalls reached its maximum throughput at lower rate compared with the TCP traffic scenario. This explains why increasing the load from 10,000 packet to 30,0000 packets did not cause a tangible increase in the throughput.

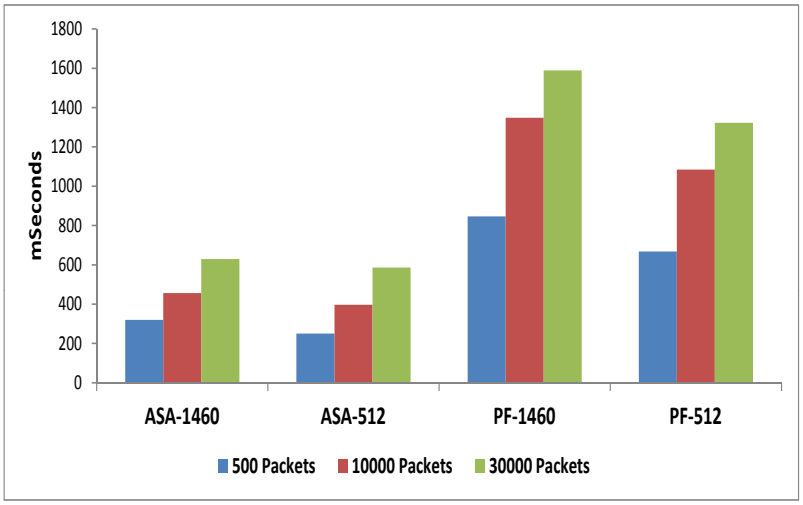

Figure 6. Delay of Network Firewalls with TCP

Figure 6 shows the end-to-end delay (in milliseconds) with TCP traffic for ASA and packet filter firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. For the same load and packet size, the figure shows that PF firewall has significantly higher delay compared to ASA firewall. In this case, both firewalls are configured with similar settings and obviously ASA outperformed PF. For all cases, increasing the traffic load obviously increases the delay and packets with 1460 result in higher delay.

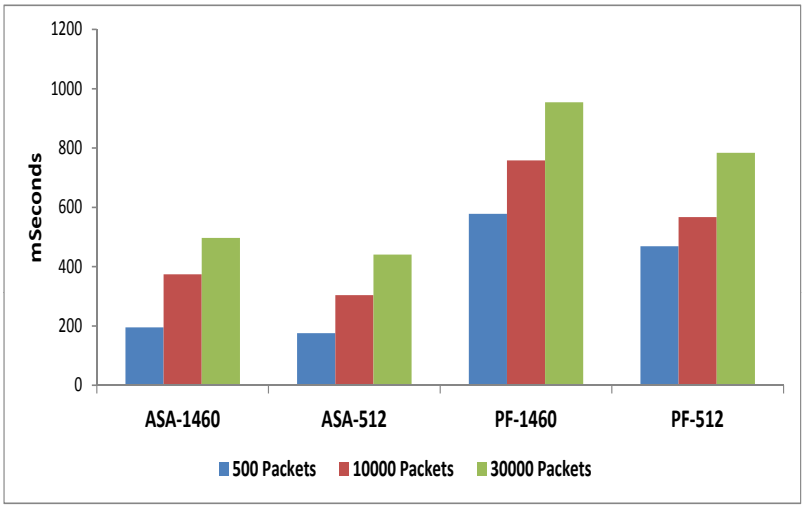

Figure 7. Delay of Network Firewalls with UDP

Figure 7 shows the end-to-end delay (in milliseconds) with UDP traffic for ASA and packet filter firewalls with packet sizes 1460 and 512 bytes and with three different traffic

loads. As shown in the figure with UDP traffic the firewalls experience a lower delay compared to TCP traffic. This can be explained that with UDP the packets are either received or lost, there is no retransmission delay after timeout as with TCP.

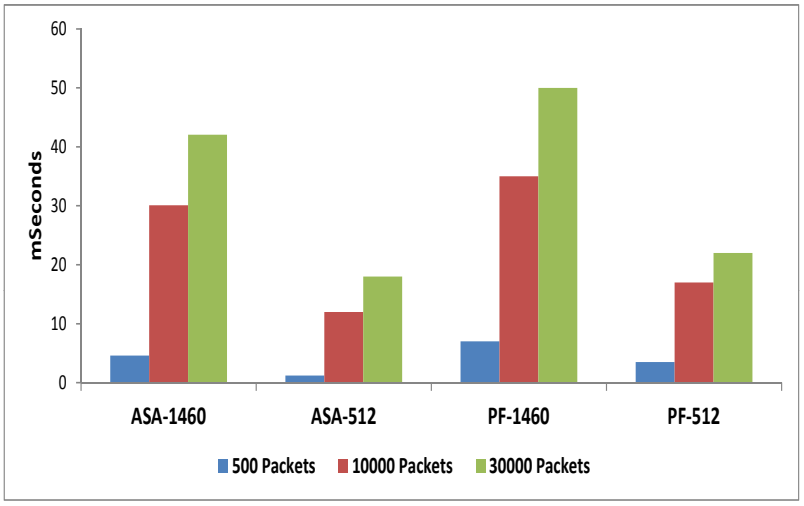

Figure 8. Jitter of Network Firewalls with TCP

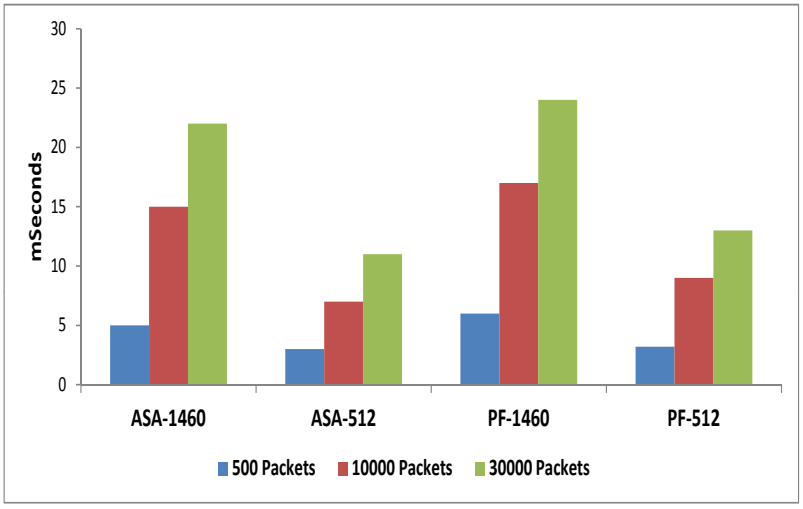

Figure 9. Jitter of Network Firewalls with UDP

Figures 8 and 9 show the jitter delay (in milliseconds) with TCP and UDP traffic for ASA and PF firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. In all cases, the figures show that the jitter increases as the load increases. Both firewalls has significantly lower jitter with UDP traffic compared to TCP traffic and packets with 1460 bytes result in higher jitter. Again, this is explained by the retransmission and timeout management mechanisms used in TCP.

Figure 10 shows the percentage of packet loss with UDP traffic for ASA and packet filter firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. The figure shows that for the same load and packet size, ASA firewall has significantly lower

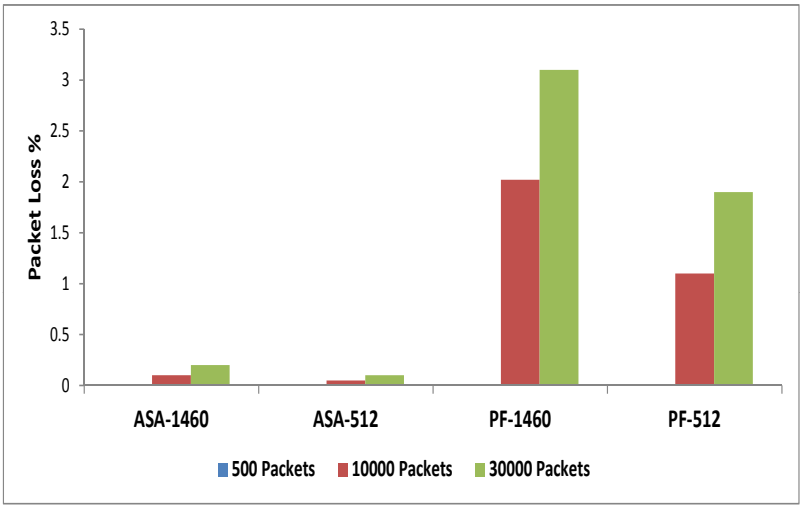

Figure 10. Packet Loss Ratio of Network Based Firewalls with UDP

packet loss percentage compared to PF. This could be related to the slower processing speed at the PF which causes the buffers to overflow, resulting in a higher packet loss ratio. In all cases, with light traffic load there was no packet loss and packets with 1460 bytes result in higher packet loss ratio. On the other hand, the packet loss was also examined with TCP traffic and the firewalls showed very low or negligible packet loss ratio.

6.2: Personal Firewalls

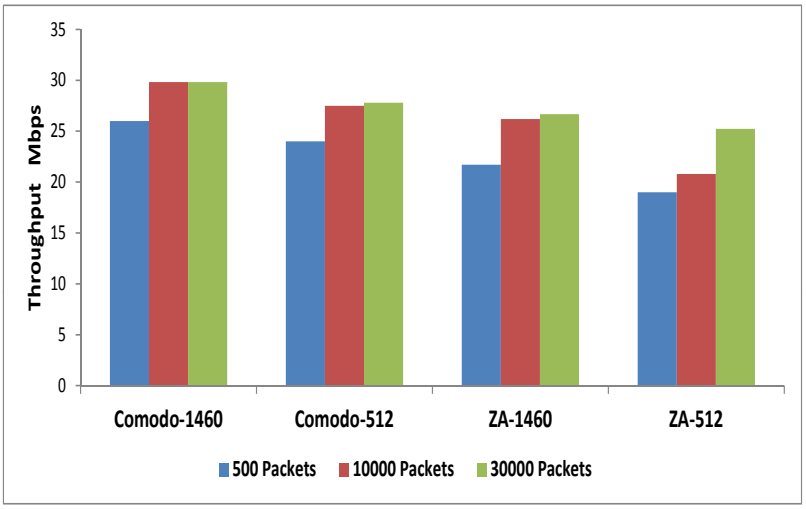

Figure 11. Throughput of Personal Firewalls with TCP

Figure 11 shows the throughput in Mbps with TCP traffic for Comodo and ZA firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. The figure shows that for the same load and packet size,the Comodo firewall has a slightly higher throughput compared to ZA. In all cases, the throughput is significantly lower than that for the network-based firewalls. This result confirms the fact that network-based firewalls

are more suitable for large networks with high traffic rates. Figure 11 shows that the throughput did not increase when the traffic load increases from medium to high, as it has reached its maximum value.

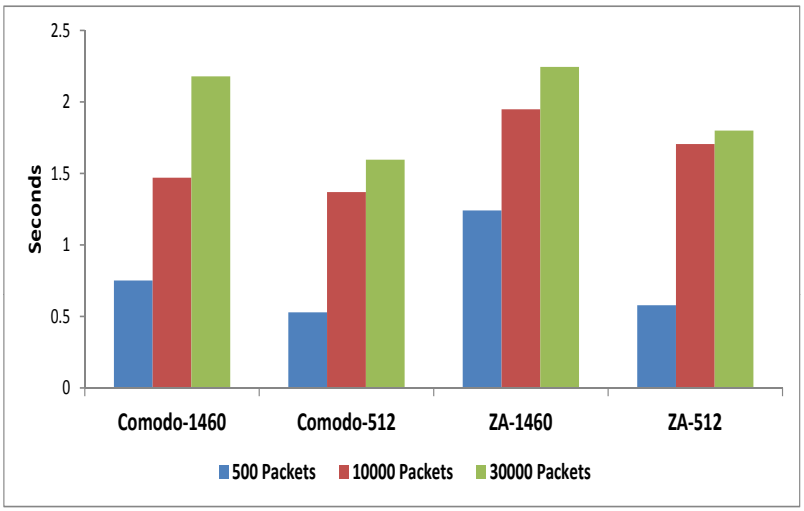

Figure 12. Delay of Personal Firewalls with TCP

Figure 12 shows the end-to-end delay (in seconds) with TCP traffic for Comodo and ZA firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. For the same load and packet size, the figure shows that software firewall has significantly higher delay compared to network-based firewall. In all cases, increasing the traffic load increases the delay and packets with 1460 result in higher delay.

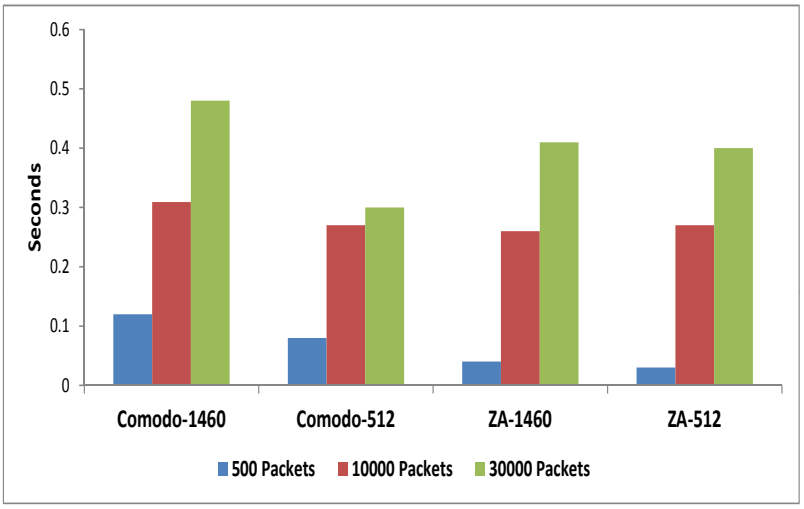

Figure 13. Jitter of Personal Firewalls with TCP

Figures 13 shows the jitter delay (in seconds) with TCP traffic for Comodo and ZA firewalls with packet sizes 1460 and 512 bytes and with three different traffic loads. For all the cases, the figure shows that the jitter increases as the load in the network increases. For the same load and packet size, the figure shows that software firewall has significantly

higher jitter compared to network-based firewall and packets with 1460 bytes result in higher jitter.

7: Security Evaluation Results

This section presents the results for the security testing of various types of firewalls. As discussed earlier, the firewalls are tested against several common security attacks. The following attacks [3, 18] are considered for the security analysis:

DDoS TCP-SYN flood attack: the aim of this attack is to flood the victim with a large number of SYN requests. The server replies with a SYN-ACK message and saves the state of the connection waiting for the final ACK, that will never arrive from the client. Servers have a finite number of connections both completed and uncompleted that could be saved, after which other SYN requests are discarded. The attacker keeps flooding the server with SYN requests from faked (spoofed) IP addresses making it unable to respond to legitimate requests.

ARP Poison attack: in this attack the adversary sends a bogus ARP reply message causing the user to mistakenly update his ARP cash table.

Man-in-the-Middle attack: the attacker in this case stealthy eavesdrops and relay packets exchanged between two parties. The result is that the attacker either identify the session key that will be used between the two parties or share a key with each party and actively relay packets which may be possibly modified.

Port scanning: is a technique in which the attacker finds open ports to discover the services they run. The aim is to try to breach into the a service.

Password Sniffing: the idea is to capture all packets and read passwords if they are transmitted in plain-text. Most FTP applications are vulnerable to this attack.

DNS Cache Poisoning Attack: in this attack the DNS at the user computer is made to cache false information [9]. After sending a DNS request computers usually accepts a reply that matches their request. The attacker injects a false DNS reply poisoning the DNS cache at the user's computer. The aim of the attacker is to guide the user traffic to fake websites of his choice causing social engineering attack [15].

TCP session poisoning: also known as TCP session hijacking which abuses the fact that, in most systems, authentication is only performed at the session setup stage. The attacker in this case impersonates the server by interjecting an already started session with a client. It requires spoofing the IP address of the server and determining the sequence number expected by the client.

Ping of death: the size of a ping packet is normally 84 bytes including the IP header. In this attack, the packet is sent in a size that exceeds the maximum limit of a packet (which is 65,535 bytes). The aim is to crash the target machine and cause a denial of service. The large packet is sent fragmented by the attacker and when reassembled at the target computer its size becomes greater than 65,536 bytes.

Teardrop Attack: this is a denial of service attack that exploits the fragmentation issues in TCP/IP. Large packets are fragmented and some information are added to the fragments to facilitate the reassembly process at the destination host or router. The attacker in this case falsifies the fragmentation information causing empty and overlapping fragments which causes the system to crash.

Some of the above attacks were implemented using available tools such as: NMAP,

Table 2. Security Tests Results

Attack Type	**ZA**	Comodo	Windows7	ASA	**PF**
DDoS-TCP-SYN	F	F	F	P	F
ARP Poison	F	F	P	P	S
Man-in-the-Middle	S	S	S	NA	NA
Port Scanning	F	P	P	NA	NA
Password Sniffing	F	F	F	NA	NA
DNS Poisoning	P	F	F	P	S
TCP session poisoning	P	P	F	NA	NA
Ping of death	P	P	F	P	S
Teardrop Attack	S	P	F	F	NA

HPING3, ETTERCAP, Wireshark and ZERO'Z Server Attack. The attacks were performed on: ZoneAlam, Comodo, Windows 7, Cisco ASA, and packet filter firewalls and the results are shown in Table 2. If the attack succeeds, the firewall is considered to fail the test (**F**). Otherwise, if the attack fails, the firewall is considered to succeeded the test (**S**). Finally, if the attack partially succeeds, the firewall partially fails the test (**P**). Some attacks are not applicable (NA) on particular types of firewalls. The results show that none of the firewalls can completely defend against all the attacks. Moreover, for the applicable attacks network-based firewalls showed a slightly better results compared to personal firewalls. Finally, built-in firewalls (e.g. Windows 7) failed in most of the performed attacks.

8: Firewalls Use and Awareness

A questionnaire was constructed by a panel of researchers in computer engineering to explore firewall use among college students at the Hashemite University. Particularly, the following questions were asked:

1. Do you have an activated Firewall on your computer or network?
2. Are you using a specialized Firewall (ex. ZoneAlarm or any Cisco firewall)?
3. Are you using a built-in Firewall (Windows or Linux)?
4. Did you do the firewall configuration yourself?

Participants had to answer with 1 = "Yes"; 2 = "No"; 3 = "I do not know". Participants filling the questionnaire were a convenient sample of 335 college students. A total of 51.9% of the sample was studying a computer-related discipline, and the rest of the sample was of other disciplines in the university. Almost 50% of the sample was senior students.

Descriptive Statistics were applied using the Statistical Package for Social Sciences software (SPSS) version 16.0 to analyze the collected data. The results showed that only 54.2% of the samples activates the Firewall on their computers and surprisingly 25.1% of the samples does not know if they have an activated firewall on their computers or networks.

Figure 14 shows the usage of specialized firewalls among students studying computer-related and other disciplines. The results show that only 12.7% of the sample use a specialized firewall and 65.9% of which are students studying computer-related disciplines. Surprisingly, 61.3% of the sample does not know if they have specialized firewalls with the percentage of students studying computer-related disciplines being slightly higher. The

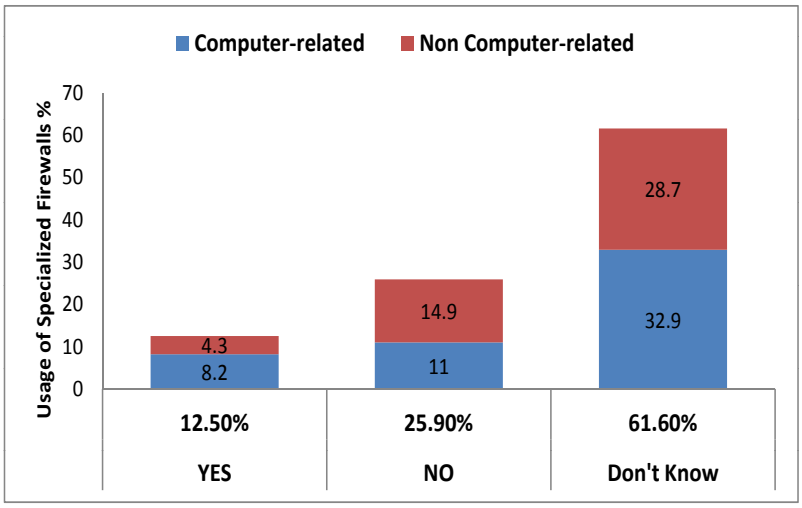

Figure 14. Usage of Specialized Firewalls

results clearly indicate that there is limited usage of firewalls and lack of awareness regarding the importance of specialized firewalls among college students. On the contrary, as for anti-virus software, most of the students were aware of their existence and importance. This is an interesting result given the fact that college students use their computers for long periods of times as part of their studies and are expected to be aware of ways to protect their computers other than conventional anti-virus software.

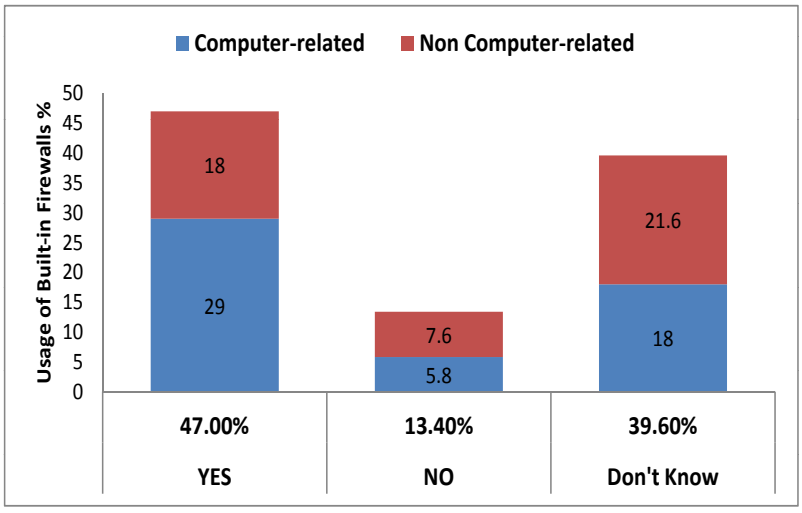

Figure 15. Usage of Built-in Firewalls

Figure 15 shows the usage of built-in firewalls among students studying computer-related and other disciplines. Only 46.8% of the sample uses a built-in firewall and 61.7% of which are students studying computer-related disciplines. Again, this indicate the lack of awareness regarding the importance of firewalls. Built-in firewalls are usually implicitly installed and activated with most of the new operating systems (e.g. Windows 7, Vista, 8 and Unix-like OS).

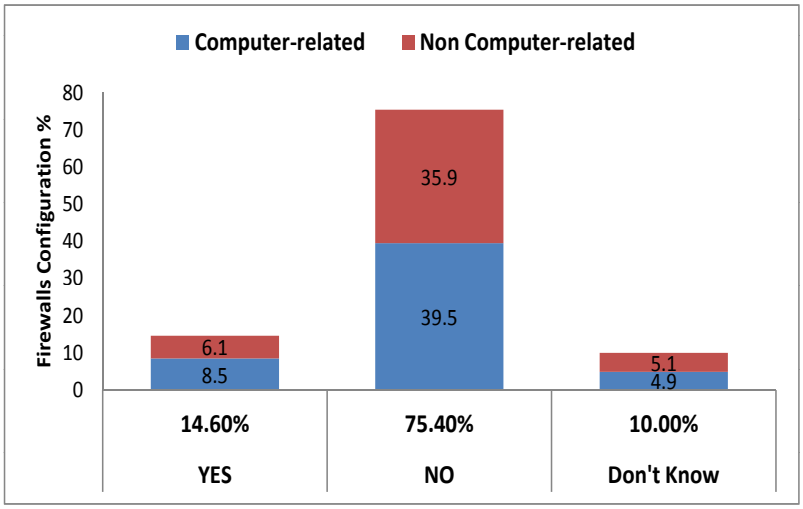

Figure 16. Firewalls Configuration

Figure 16 shows the firewalls configuration among students studying computer-related and other disciplines. Only 14.5% of the sample configures their firewalls. This implies that most of the users simply install their firewalls without any configuration and expect them to operate efficiently similar to anti-viruses. There were no significant differences between students of computer-related disciplines and others. Unfortunately, most of the attacks against firewalls (as discussed in Section 7) require computer users to carefully configure their firewalls to guarantee network security. Leaving firewalls on default settings, or without adjustment, may allow malicious connections on a computer which comprises security.

9: Conclusion and Future Research

Firewalls are considered an essential part of any information security system. They are the first defense line against any cyber attack. In this paper, we presented an assessment methodology to analyze the performance of different firewalls platforms. The performance analysis considered delay, jitter, throughput, and packet loss. The proposed methodology was tested by performing a number of experiments on different types of firewalls including network-based and personal firewalls. The results showed that network-based firewalls outperformed personal firewalls in all metrics and Cisco ASA achieved better performance than packet filter. Moreover, the security of the firewalls was tested by applying a set of attacks and observing the reaction of the firewalls. The results showed that not all the firewalls can protect against the proposed attacks, which confirms the idea of using both personal and network-based firewalls to provide layered security. Other results in this study showed that most computer users do not use or configure firewalls on their devices which is a concerning issue for network administrators. In future research, we plan to consider other attacks and test the firewalls individually and combined, i.e. both personal and network-based, against these attacks. Additionally, we plan to design and test FPGA-based firewalls as they are expected to provide high performance, particularly in terms of delay and throughput.

References

[1] Atomtime. http://www.atomtime.com/. Accessed: 2013-04-22.

[2] Cisco systems, inc. http://www.cisco.com. Accessed: 2013-04-22.

[3] Common vulnerabilities and exposures. http://www.cve.mitre.org/. Accessed: 2013-04-28.

[4] Ip traffic. http://www.zti-telecom.com/. Accessed: 2013-04-22.

[5] M.Z.A. Aziz, M.Y. Ibrahim, A.M. Omar, R. Ab Rahman, M.M. Md Zan, and M.I. Yusof. Performance analysis of application layer firewall. In *In Proc. of IEEE ISWTA*, pages 182–186, 2012.

[6] Shuo Chen, Jun Xu, Zbigniew Kalbarczyk, Ravishankar K Iyer, and Keith Whisnant. Modeling and evaluating the security threats of transient errors in firewall software. *Performance Evaluation*, 56(14):53 – 72, 2004.

[7] A. El-Atawy, T. Samak, E. Al-Shaer, and Hong Li. Using online traffic statistical matching for optimizing packet filtering performance. In *In Proc. of IEEE INFOCOM*, pages 866–874, 2007.

[8] Mohamed G. Gouda and Alex X. Liu. Structured firewall design. *Comput. Netw.*, 51(4):1106–1120, March 2007.

[9] A. Householder, K. Houle, and C. Dougherty. Computer attack trends challenge internet security. *Computer*, 35(4):5–7, 2002.

[10] Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting browsers from dns rebinding attacks. *ACM Trans. Web*, 3(1):2:1–2:26, January 2009.

[11] A.X. Liu and M.G. Gouda. Diverse firewall design. *Parallel and Distributed Systems, IEEE Transactions on*, 19(9):1237–1251, 2008.

[12] G. Misherghi, Lihua Yuan, Zhendong Su, Chen-Nee Chuah, and Hao Chen. A general framework for benchmarking firewall optimization techniques. *IEEE Trans. on Netw. and Serv. Manag.*, 5(4):227–238, December 2008.

[13] S. Nassar, A. El-Sayed, and N. Aiad. Improve the network performance by using parallel firewalls. In *In Proc. of IEEE INC*, pages 1–5, 2010.

[14] D Newman. *Benchmarking Terminology for Firewall Performance*. IETF RFC 2647, 1999.

[15] Marcus Rogers. *Social Engineering: Mitigation*, chapter 330, pages 2751–2760. Taylor and Francis, 2011.

[16] K. Salah, K. Elbadawi, and R. Boutaba. Performance modeling and analysis of network firewalls. *IEEE Transactions on Network and Service Management*, 9(1):12–21, 2012.

[17] C. Sheth and R. Thakker. Performance evaluation and comparative analysis of network firewalls. In *In Proc. of IEEE ICDeCom*, pages 1–5, 2011.

[18] William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 5th edition, 2011.

[19] Lihua Yuan, Hao Chen, Jianning Mai, Chen-Nee Chuah, Zhendong Su, and P. Mohapatra. Fireman: a toolkit for firewall modeling and analysis. In *In Proc. of IEEE Symposium on Security and Privacy*, pages 15 pp.–213, 2006.

Thaier Hayajneh received his Ph.D. and M.Sc. degrees in Computer and Network Security from the University of Pittsburgh, PA, USA in 2009 and 2005, respectively. He also received his M.Sc. and B.Sc. in Electrical and Computer Engineering from Jordan University of Science and Technology, Irbid, Jordan, in 1999 and 1997, respectively. He is currently Chair and Assistant Professor in the Computer Engineering Department at the Hashemite University, Zarqa, Jordan. His current research interests include: computer networking (including mobile wireless ad hoc and sensor networks), information assurance and security, network security and privacy, wireless security, and system modeling and simulation.

Bassam J. Mohd received his B. S. in Computer Engineering from the KFUPM of Dhahran-KSA, his M. S. in Computer Engineering from the University of Louisiana at Lafayette and his PhD from

the University of Texas- Austin, 2008. He has worked for several semiconductor companies including Intel, SUN, Synopsys and Qualcomm. He is currently an assistant professor at the Hashemite University, Jordan. His research interest includes DSP designs, Steganographic processors, Encryption processors and power reduction/estimation techniques.

Awni Itradat received the B.SC. degree in Computer Engineering from Jordan University of Science and Technology, Jordan in 2000, and the Master and Ph.D. degrees in Computer Engineering from Concordia University, Montreal, Canada in 2008. He is currently an Assistant Professor in the Department of Computer Engineering, Hashemite University. In 2009, he was appointed as the chairman of the Department of Computer Engineering at the Faculty of Engineering in the Hashemite University. He has also served as a Director of the Computer Center in Hashemite University and, currently, working as the director of the ICT and E-learning Center in the Hashemite University. His research interests include Computer Architecture and Networks, Design of VLSI circuits and systems, Interconnect Modeling and Design, Reconfigurable Circuits, High Level Synthesis of 3D- and 2D-Circuits and Systems.

Ahmad Nahar Quttoum received his Ph.D. degree in Computer Networks from the University of Quebec, Montreal, Canada. In late 2007, he received his M.Sc. degree in Network Systems from the University of Sunderland, UK. From Jordan University of Science and Technology, in 2006, he received the B.Sc. degree in Computer Engineering. Currently, he holds an Assistant Professor position in the Department of Computer Engineering at the Hashemite University (HU), Jordan. Before joining the HU, he worked as a Post-Doctoral researcher at the UQAM, Montreal, Canada. His research interests include cloud computing, data center networks, virtualized networks, autonomic resource management, and network security.

