International Journal of Computer Sciences and Engineering
Vol.**11**, Issue **4**, pp.**01-06**, April **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

IJCSE
ISSN: 2347-2693 (E)

Research Paper

A Framework for Reducing the Cost of the Firewall

Mohammed Alwajeeh[1*], Saleh Noman Alassali[2], Yasser Ali Alahmadi[3]

[1,2,3]Dept. Computer Science, Saba Region University, Marib, Yemen

**Corresponding Author: mohammedsharaf32@gmail.com. Tel.: +967-770447076*

Received: 25/Feb/2023; **Accepted**: 05/Apr/2023; **Published**: 30/Apr/2023. | **DOI**: https://doi.org/10.26438/ijcse/v11i4.16

Abstract - Today, the world has become like a small village, and the success of any institution has become closely related to communication with the outside world through the Internet. As each institution needs to exchange information from one place to another that exposes sensitive information to danger and spread. Such institutions require the existence of mechanisms to protect this information. The firewall plays an important role in protecting information from unauthorized access. However, the available firewalls are not suitable for all institutions due to their high cost. This paper proposes a micro-firewall for reducing the cost of firewall by avoiding the additional services while maintaining the security, and thus the proposed micro-firewall will suitable the small and medium institutions. The proposed micro-firewall uses two computers, one of them is connected with the internet and the other is connected with the local network, the communication between the two computers is done by using the server and client protocols. The role of the computer connected with the internet is to receive the request from the external user who want access the internal network and verify the identity of the user if he/she is an authorized user or not. If yes it sends the request to the computer connected with the internal network, unless the request is rejected. The role of internal computer is similar to external computer but for internal user. The proposed micro-firewall was compared with other firewalls in terms of the cost reduction. The results showed that the cost of proposed micro-firewall has reduced compared with the cost of the other firewalls.

Keywords: firewall, client, server, agent, proxy, packet filtering, user filtering, network security.

1. Introduction

A firewall is one of the major technique in networks security. It is central to control the data passing between two networks (trusted) LAN and (untrusted) internet and protect institutions against cyber-attack. The firewalls work as checkpoint that allow some people to pass and prevent the others according to previous instructions.

A firewall is implemented by definite security rules, which can set up by system admin that permit valid data to get access to the required server like FTP server ,web servers, talnet servers ...etc. All the traffic between trusted and untrusted networks is monitored and governed by firewall[1].There are two types of firewalls, it may be hardware or software.Any firewall consists of a set of components and every component has a special task that acts with each other to achieve the required goal of the firewall. Every component has some advantages and disadvantages and nobody can claim extreme protection.

There are many firewalls on the market, not all of them are convenient for small and medium institutions (SMIs) due to their height cost[2],because such firewalls introduce additional services.
This paper focus on reducing the cost of the firewall by avoid additional services that the SMIs do not need it, while maintaining security for such institutions. The micro-firewall use two computers, one is connected with the internet and the other is connected with the local network. The role of external computer is to receive the requests from the external users, authenticate valid external users and work as proxy between the internal computer and the external users, while the role of internal computer is to receive the requests from internal users, authenticate valid internal users and work as proxy between the external computer and the internal users.

This paper is organized to eight sections, Introduction is in Section 1, Notations are in Section 2, Problem Description in Section 3, Review of Related Works is in Section 4, Firewall Components are in Section 5, the Proposed Micro-Firewall Framework is in Section 6, The Results and Discussion are in Section 7 and Conclusion and Future work are in Section 8.

2. Notations

The notations used to describe the framework are showed in Table 1.

Table 1.Notations

Notation	Description
U_id	Identification of user that request the service
Grp_num	Identification of group that service belong to

In_or_out	Internal or external connection
Rqst_no	is the a unique identification for request
Srv_no	A unique Identification of service
PRu	User private key
PKu	User public key
SKu	User secret key
PKx	Proxy public key
PRx	Proxy private key

3. Problem Description

With the rising number of devices that connect with SMIs networks, unforeseeable malicious attacks have risen. Make regularity between costs and technological advances has always been a balancing act, especially for SMIs IT infrastructure[3]. Despite there are different types of firewalls and security technologies in the market, not all are convenient for small and medium institutions (SMIs). For SMIs, these technologies may by destructive, both functionally and financially[2]. In such SMIs, it may have a height cost firewall introducing N services that are not commensurate with the financial power of these SMIs then the cost becomes a big problem. Therefore, the key problem in this paper is the height cost of the firewalls. Table 2 shows some deferent firewalls prices.

Table 2. Deferent Firewalls Prices

No	Firewall Description	Price
1	7-port SonicWall TZ400 - Security appliance - 7 ports - GigE	$945.00
2	Cisco Firewall ASA5506 with Subscription L-ASA5506-TAMC-1 Year	$1,275.60
3	Cyberoam 35iNG with 1 year license (For 70 User)	$1,314.68
4	ASA 5505 Sec Plus Appliance with SW. UL Users. HA. 3DES/AES.	$1,695.00
5	SONICWALL TZ500 WITH 1YR TOTALSECURE	$1,865.00
6	Cyberoam 50iNG with 1 year license	$2,127.77
7	Cisco ASA 5516-X with FirePOWER services, 8GE, AC, 3DES/AES with 3YR FirePOWER services	$3,069.56
8	Cisco ASA5508 FirePOWER IPS, AMP and URL 3YR Subs	$3,566.86
9	ASA 5512-X with SW. 6GE Data. 1GE Mgmt. AC. NPE	$3,995.00
10	SonicWall NSA 4650 High Availability - Security appliance - 10 GigE, 2.5 GigE - 1U - rack-mountable	$4,545.00
11	ASA 5515-X with SW. 6GE Data. 1GE Mgmt. AC. NPE	$4,995.00
12	ASA5520 Appliance w/DCpower,SW,HA,4GE+1FE,DES REMANUFACTURED	$5,517.00
13	Fortinet FortiGate 500E - UTM Bundle - security appliance - with 1 year FortiCare 24X7 Comprehensive Support + 1 year...	$9,841.99
14	ASA 5540 Appliance with SW, HA, 4GE+1FE, DES REMANUFACTURED	$10,197.00
15	ASA5550 Appliance w/SW, HA, 8GE+1FE,DES REMANUFACTURED	$11,997.00
16	Fortinet FWB-2000E Web Application Firewall - 2 x 10GE SFP+ ports, 4 x GE RJ45 bypass ports, 4 x GE SFP ports, dual AC power supplies, 2 TB storage	$44,000.00
17	Fortinet FWB-3000E Web Application Firewall - 4 x 10GE SFP+ ports, 8 x GE RJ45 bypass ports, 4 x GE SFP ports, dual AC power supplies, 4 TB storage	$91,994.25
18	Fortinet FWB-3010E Web Application Firewall - 8 x GE RJ45 bypass Ports, 4 x GE SFP Ports, 2x 10G SFP+ bypass ports, 2x 10G SFP+ ports, dual AC power supplies, 2 x 2TB HDD Storage	$114,994.25
19	Fortinet FWB-4000E Web Application Firewall - 8 x GE RJ45 bypass Ports, 4 x GE SFP Ports, 2x 10G SFP+ bypass ports, 2x 10G SFP+ ports, dual AC power supplies, 4 TB storage	$172,494.25

4. Related Work

The first firewall has suggested since about 1987, and several studies have already been proposed. The author in[4], proposed a new model to choose the most convenient firewall and the estimates are finished agreeing with proposed new model, The results show that the proposed model and the criteria can be used to evaluate and choose the best alternative of firewall.

The author in [5], introduced two models to find out web application flows using a group of web vulnerability scanners applications (Python based scanners) and using Web based Firewall called ModSecurity to reduce vulnerabilities.

The authors in [6], tested the network security threats, policies, and mechanisms as well as analysed the firewall as a network masking technology by using Netfilter/Iptables as an implementation technique. For evaluation, the authors consider two sides, the routing and the security. The results showed that IPtables is efficient and trustworthy.

The authors in [7], developed a configurable software-based firewall(P4Guard) using a language called p4 to determine packet processing logic. To prove the efficiency of P4Guard the authors compared the P4Guard with a ClickOS-based virtual firewall called VNGuard. The comparison study included many sides as programming language used to develop, configurability, flexibility and for evaluation, the authors use terms time of packet processing and time of round trip using different configurations in Cloud Lab. The experimental results showed that the P4Guard has fast time in packet processing and for small packet the network latency was low.

The authors in [8], suggested enterprise firewall virtualization design for Grid that operated as a set of security components. The firewall virtualization framework included an firewall device that separate the Grid resources network from the outside, a firewall agent that introduce firewall running depend on Authentication, Authorization, and Accounting (AAA), and a front-end machine to receive credentials provided by Grid clients.

The authors in [9], reviewed the historical violation of the next generation firewall. The information in this paper showed how intrusion detection, analysis, and response can

be done by NGFWs. Finally, useful techniques and tips on how to benefit from NGF were also presented.

The authors in [10], analysed many types of open-source firewalls. The results showed that pfsence is the most integral open source firewall obtainable on the market and a firewall to secure web applications that use the same mechanism in the host-based firewall, as well as the study showed ModSecurity is the best system of WAF that exists with many of capacities and properties

The authors in [11], used Software-Defined Networking to suggest a framework for security services and determined the prerequisites for that framework. They suggested a firewall and attack mitigate as two security representatives.

Liu, Dou et al in[12], suggested a secured cloud firewall framework to save the cost of resources and established a new model based on the theory of queuing for the performance analysis of the suggested cloud security firewall, where times of firewall service are modeled to go after the geometric distribution. The results showed that the expanded simulations ensure that M/Geo/1 is better than traditional M/M/1 in representing the cloud firewall real system. In addition, it is possible to configure a firewall for independent services that are hosted in the cloud for customers at reasonable prices.

5. Firewall Components

There are many types of firewalls, it may be hardware or software. However, any firewall consists of a set of components and every component has a special task, which is attractive with each other to achieve the required goal of the firewall. According to[13, 14] the basic firewall components and technologies are:

5.1 Packet Filtring

The general proposition of this component is to determine if the packet is suspected or not. This component checks every packet that sent to access the internal network. But it does not check the whole packet it only checks packet header parts[15, 16] as source IP, destination IP,TCP and UDP ports. Packet filtering can be divided into two types, stateless and stateful. In stateless packet filtering of the firewall, decide whether to permit or reject a packet by checking all packet header parts. On the other hand, stateful packet filtering is a promoted version of the stateless filtering mechanism. The main difference is that stateful packet filtering keeps the state of all connections across the firewall in memory, and decides if to drop independent packets using that saved state

5.2 Proxy Server

The main reason behind developing proxy servers was to save web pages that were accessed repeatedly[13]. This component works in the application layer[13, 17, 18] as well as work behalf of the original server, where it receives the requests and examines the requests according to the policy set by the institution, and based on the result of the examination, the appropriate decision is taken, if the result of the examination is under the required rules, the delivery request is made by the agent on behalf of the original or rejects the delivery request completely . In most firewalls, this component performs most functions, as it contains multiple application systems.

5.3 Network Address Translation

Network Address Translation (NAT) is the mechanism that is proposed to solve IP address consumption [18]. NAT change local IP addresses in the LAN network to globally unique public IP addresses to use on the internet. Each NAT device has a table consists of couples of local IP addresses and globally alone public IP addresses[18]. All traffic on local network shows to the internet comes from one computer. Many firewalls back different types of NAT but not any firewall back every type of NAT.

5.4 Virtual Private Network (VPN*)*

If you want to stretch your LAN through the internet to remote client computers or remote networks you can use Virtual Private Networks (VPNs)[13]. VPNs envelop the LAN traffic in IP packets to direct LAN traffic from one local network to another by using the internet. Connecting to an ISPs that back VPN protocol or VPN software installed on client computers helps the client to have a VPN service. The issue of straight internet access to servers solved by Virtual Private.

6. Proposed Micro-Firewall Framework

This paper aims to build a micro-firewall framework that convenient the small and medium institutions by reducing the number of additional services, Figure 1 explores the proposed micro-firewall framework.

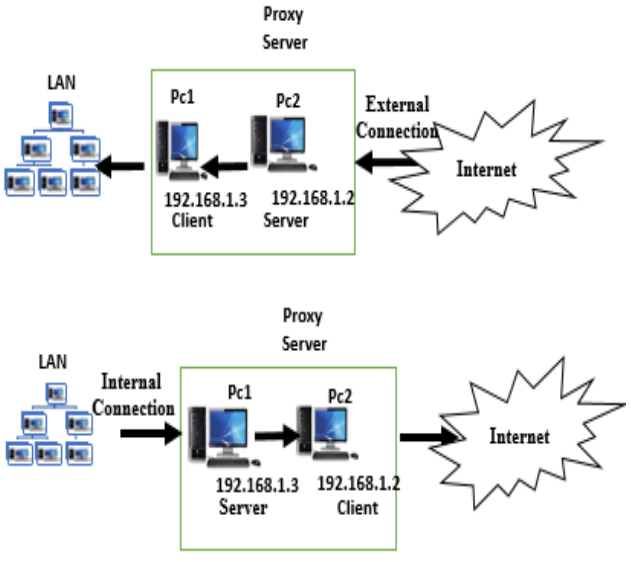

Figure 1 . The Proposed Micro-Firewall Framewok

In the proposed micro-firewall, instead of use source IP, destination IP and ports number as in traditional firewalls to build firewall rules, the users information is used to identify the users. Therefore, this proposed micro-firewall consists of three components: user registration, user filtering and proxy server.

6.1 User Registration

When a new user requires any service from the institution for the first time, the request will be received by the proxy server, the proxy server will ask the user to send his/her information like user name, birthday ….etc. Then the creation of user account occurs only one time. The Figure 2 illustrates registration process and the steps of this process are as follows:

1. The user sends his/her information profile to proxy server.
2. Proxy server saves a copy of the user information, distributes the user to the suitable group of the services to produce user_text1, after that, the proxy server sends the public algorithm to the user to generate his /her public/private keys.
3. The user receives the public algorithm, generates his public/private keys and then he/she sends his/her public key to the proxy server.
4. Proxy server hashes the user_text1 using its master key to produce user secret key. After that, the proxy server encrypts the user secret key using the user public key and sends the result to the associated user.
5. The user receives the message, decrypts it by using his/her private key to retrieve his/her secret key.

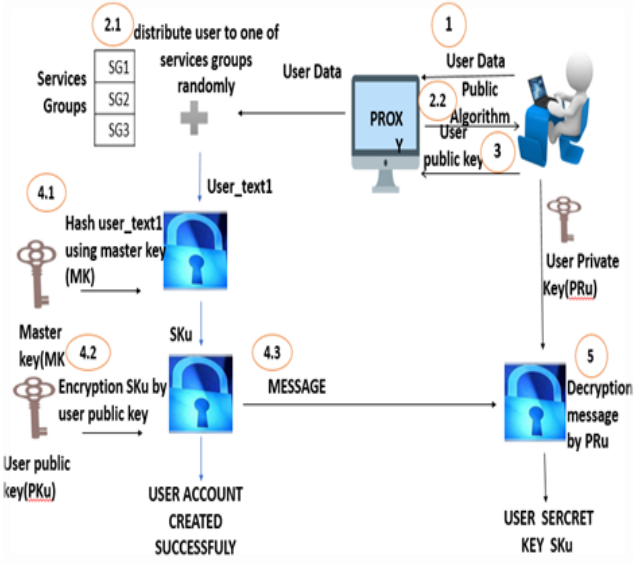

Figure 2. User Registration Process

6.2 User Filtring

In the proposed micro-firewall, the user must be registered with the institution and has account. When the user tries login and access to the institution services, the following filtering process steps occurs:

1. User sends a service request to proxy server.
2. Proxy server receives the user request and checks if the associated user has account or not if yes .proxy server generate a random number R1, signs it using its private key. After that, it appends the signed message with R1, encrypts the result using SKu and sends it to the user.
3. The user receives the message, decrypts it using his/her SKu to retrieves the singed message and R1. After that, he decrypts the singed message using PKx and then he compares the R1 with the decrypted signed message, if match, go to the step 4, otherwise, end connection
4. The user signs the R1 using his/her private key, encrypts the result using proxy public key and sends the encrypted message to proxy server.
5. Proxy server receives the message and decrypts it using its private key, gets the signed message by user. After that, it decrypts the signed message using PKu. Then it match the result with R1 that it generate in step 2. If true, it starts to execute the user request by applying the proxy service, else login failed.

6.3 Proxy Server

In this component the micro-firewall achieve the proxy process. The proxy server have list of services that allow the user to choose from it, the request queue, the log file and the distributed database that contains users information. The log file will contain all log events to the proxy server. This framework depend basically on two computers pc2 and pc1. In this component, the pc2 takes the proxy role if the connection request was coming from out institution (external) while the pc1 takes the proxy role if the connection request was coming from inside the institution (internal). However, after user passed the log in process, one of the following scenarios must be performed based on type of connection.

6.3.1 External Connection

In this scenario, the request will come from external user and the following procedure will perform**:**

- PC2 will send the request service of user to PC1 encrypted by PKc1. The request includes: u_id, grp_num, srv_no, and rqst_no.
- PC1 receives the encrypted request, decrypts it using its PRc1 and prepares the result of request and sends back to PC2 encrypted by PKc2. The result includes: u_id, grp_num, srv_no, rqst_no and data.
- PC2 receives the encrypted message, decrypts it using its PRc2 and encrypts the result using SKu and sends it to the user.

6.3.2 Internal Connection

In this scenario, the request will come from internal user, the following procedure will perform**:**

- PC1 will send the request service of user to PC2 encrypted by PKc2. The request includes: u_id, grp_num, srv_no, and rqst_no.
- PC2 receives the encrypted request, decrypts it using its PRc2 and prepares the result of request and sends back to PC1 encrypted by PKc1. The result includes: u_id, grp_num, srv_no, rqst_no and data.
- PC1 receives the encrypted message, decrypts it using it's PRc1 and encrypts the result using SKu and sends it to the user.

7. Results and Discussion

This section compares the proposed micro-firewall with others in term the cost and discusses the results. In this paper, we do not consider another factor such as performance, due to

the purpose of this paper is for reducing the cost. However, the cost of micro-firewall is compared with the cost of others firewalls. The cost depended basically on number of services supported in each firewall, the table 3 below shows some firewalls and security services supported in each one. In this comparsion we use four security services to compare the proposed micro-firewall with others.

Table 3. Firewalls Services Comparison

Firewalls	Supported Services			
	PACKET FILTRING	VPN	NAT	PROXY
Whatcgurd[19]	√	√	√	√
poloalto[20]	√	√	√	√
FORTINET[21]	√	√	√	√
Juniber[20]	√	√	√	√
Untangle[22]	√	√	√	√
Suggested micro-firewall	√	×	×	√

From Table 3 above we can note, in the proposed micro-firewall the services have been reduced from four to two services. These two services will perform the operations of all services due to the proposed micro-firewall uses user filtering instead of packet filtering to facility the access to the institution from any device, as well as it uses the proxy to hide the internal network host that means the proposed micro-firewall provides NAT within proxy service.

The Table 4 show the compression of cost between the proposed micro-firewall and others. Suppose the firewall have N of services like packet filtring, NAT, proxy, vpn …..etc and let S refers to the services S1, S2, S3, S4 ….Sn and C refers to the cost. Here we suppose the cost is same for each service, so the total cost = C*N

While N is the number of services and the C is the cost of each service. In the comparison we have four services and suppose the cost of each service will be $100, so the cost of firewall supported all services will be $400.

Table 4. Firewall Cost Comparison

Firewalls	Supported Services				Total Cost
	PACKET FILTRING	VPN	NAT	PROXY	
Whatcgurd[19]	$100	$100	$100	$100	$400
poloalto[20]	$100	$100	$100	$100	$400
FORTINET[21]	$100	$100	$100	$100	$400
Juniber[20]	$100	$100	$100	$100	$400
Untangle[22]	$100	$100	$100	$100	$400
Suggested micro-firewall	$100	$0	$0	$100	$200

The Figure 3, show the results of comparison between proposed micro-firewall and others. The results showed that the cost of the firewall is directly proportional to the services it provides and the services reduced from four to two. Therefore, the proposed micro-firewall has lowest cost than the others due to the number of services it provides which causes reducing the cost of the proposed micro-firewall**.**

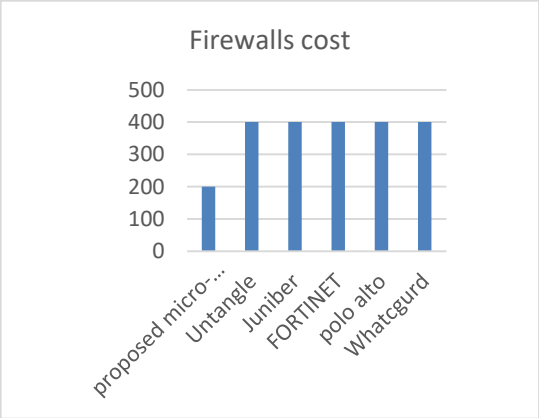

Figure 3. Firewalls Cost Comparison

8. Conclusion and Future Scope

This paper has focused on the high cost of firewall problem and has proposed a micro-firewall to reduce the cost of firewall by avoiding some services and thus, the proposed micro-firewall will suite the small and medium institutions that cannot buy the available firewalls in the markets. The proposed framework has used the user filtering instead of IPs and ports filtering. Therefore, some of services are ignored such as NAT, VPN that depend on IPs address as result of the proposed micro-firewall has reduced the main services from four into two services as shows in Table 3. The proposed micro-firewall has been compared with others in terms of the cost. The comparison results showed that the proposed micro-firewall has lowest cost than the others.
The futures work may be performed by investigating IDs service of the proposed framework and improving the framework to hold this service.

References

[1] N. Sultana, "A Framework of Wireless Network Security Threats: Solution for Various Information Security Problems," 2019.
[2] K. C. Patel and P. Sharma, "A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization," *IJARIIE*, vol. 3, pp. 2395-4396, 2017.
[3] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME)," *Future Internet*, vol. 13, p. 186, 2021.

[4] C. Akturk and C. Cubukcu, "A Decision Making Model Proposal for Firewall Selection," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, pp. 3588-3607, 2021.

[5] T. Jain and N. Jain, "Framework for Web application vulnerability discovery and mitigation by customizing rules through ModSecurity," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2019, pp. 643-648.

[6] M. Mihalos, S. Nalmpantis, and K. Ovaliadis, "Design and Implementation of Firewall Security Policies using Linux Iptables," *Journal of Engineering Science & Technology Review*, vol. 12, 2019.

[7] R. Datta, S. Choi, A. Chowdhary, and Y. Park, "P4guard: Designing p4 based firewall," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pp. 1-6, 2018.

[8] A. Sujarwo and J. Tan, "Enterprise firewall virtualization design," in *MATEC Web of Conferences*, p. 03004, 2018.

[9] J. Surana, K. Singh, N. Bairagi, N. Mehto, and N. Jaiswal, "Survey on next generation firewall," *International Journal of Engineering Research and Development*, vol. 5, pp. 984-988, 2017.

[10] D. Sampaio and J. Bernardino, "Evaluation of Firewall Open Source Software," in *WEBIST*, pp. 356-362, 2017.

[11] J. Jeong, J. Seo, G. Cho, H. Kim, and J.-S. Park, "A framework for security services based on software-defined networking," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, pp. 150-153, 2015.

[12] M. Liu, W. Dou, S. Yu, and Z. Zhang, "A decentralized cloud firewall framework with resources provisioning cost optimization," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 621-631, 2014.

[13] M. Strebe and C. Perkins, *Firewalls 24seven*: Sybex, 2000.

[14] G. Bastien and C. Degu, *CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide (CCSP Self-Study)*: Cisco Press, 2003.

[15] D. L. Shinder and M. Cross, *Scene of the Cybercrime*: Elsevier, 2008.

[16] J. R. Vacca, *Network and system security*: Elsevier, 2013.

[17] P. B. Ambhore and K. A. Wankhade, "Proxy Server FOR Intranet Security."

[18] C. L. Schuba, "On the modeling, design, and implementation of firewall technology," Purdue University, 1997.

[19] S. Pinzon, "Top 10 threats to SME data security," *WatchGuard Technologies*, 2008.

[20] A. Malmgren and S. Persson, "A comparative study of Palo Alto Networks and Juniper Networks next-generation firewalls for a small enterprise network," ed, 2016.

[21] K. Tam, M. H. H. Salvador, K. McAlpine, R. Basile, B. Matsugu, and J. More, *UTM Security with Fortinet: Mastering FortiOS*: Newnes, 2012.

[22] A. E.-M. A. El-Bawab, *Untangle Network Security*: Packt Publishing Ltd, 2014.

AUTHORS PROFILE

Mohammed Alwajeeh holds a B.Sc. in Computer Science from Taiz University in 2012. He is currently working as Technical Support Engineer in YEMENSOFT Company, Department of Customer Services. He possesses a strong passion for technology and strives to enhance his knowledge and impart expertise on various areas including network security, Data Analysis, Artificial Intelligence and Programming.

Dr. Saleh Noman Abdullah Alassali, pursed B.Sc. CE from KSU University, Saudi Arabia in 1988, M.Sc. CS from Pune University, India in 2000 and Ph.D. in Information Security from SRTM University, India in 2005. He is currently working as Associated Professor in each of Department of Computer Sciences, Saba Region University, Science and Technology University, Yemen. He has published more than 8 research papers in reputed international journals. His main research work focuses on cryptography algorithms and random number generators.

Yasser Ali Alahmadi, pursed B.Sc. CS from Sana'a University, Yemen. Heis currently pursuing Master of Computer Science, Department of Computer Science, Saba Region University, Yemen. His interest research areas: Information Security and C# Programming.

