Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 260-267
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 202

Comparison Between Stateful Inspection Firewall and Next Generation Firewall in LAN and WAN Environments

Sally A. Al-Hasnawi[1], Aws A. Abdulsahib[2], Ahmed Zeyad Almhanna[3]
[1]Department of Information technology, University of Al-nahrain, Baghdad, Iraq
[21]Department of computer science, University of Dijlah, Baghdad, Iraq
[3]Department of medical physics science, University of Dijlah, Baghdad, Iraq

Article Info

Article history:

Received: Apr.,15,2026
Revised: May,30,2026
Accepted: Aug.,19,2026

Keywords:

Stateful Inspection Firewall
Next Generation Firewall
Network Security
LAN
WAN

ABSTRACT

Stateful inspection firewall also referred to as Stateful packet inspection is a network-based firewall that individually tracks sessions of network connections traversing it, and it operates by monitoring active connections making decisions based on the state of the traffic. Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology, combining a conventional firewall with other network device filtering functions, such as an application firewall using in-line Deep Packet Inspection (DPI), an intrusion prevention system (IPS). Firewall weakness in several types of networks caused negative effects and drop down the network and broke over the privacy. We create a scenario based on TCP protocol to evaluate the efficiency of the firewall based on two main measurement elements that represent accuracy and throughput. Also, this paper provides a comparative analysis of Stateful inspection firewalls and Next Generation Firewalls (NGFWs) within Wide Area Network (WAN) Local Area Network (LAN) environments. In our work, we depend on the eclipse-java-2023 program and use Java language. The results in LAN show that NGFW is much better than the Stateful inspection firewall which gains an accuracy of 68% and throughput of 0.89 packets/ms, While in WAN NGFW i s better than the Stateful inspection firewall when using accuracy reaches 56% as performance but when using throughput Stateful inspection firewall better than NGFW reach 1.57 packets/ms.

Corresponding Author:

Aws A. Abdulsahib
Department of Computer Science, University of Dijlah
Baghdad, Iraq
Email: aws.kareem@duc.edu.iq

1. INTRODUCTION

Cybersecurity is a critical concern in the digital age, exacting innovative approaches to systems and safeguarding sensitive information [1]. A firewall looks like a barrier that supports security via filtering traffic and is a significant section of the security of any network [2]. Also, it can be of two kinds namely, host-based firewalls or network firewalls. Host-based firewalls assist in filtering traffic to the hosts or the end devices, and Network firewalls assist in supporting security among networks, and these run on network hardware [2]. Firewalls typically focused on rules that were set up statically similar to access policy lists. Over the years, with increasing threats, they have developed to dynamically react and detect to threats to the network [3]. Firewall has many types of Traditional firewall, Next Generation firewall (NGFW), Stateful inspection firewall, and Zone-Based policy firewall. Our study focused on NGFW and Stateful inspection firewall. Next-generation firewall (NGFW) merge methods such as Intrusion Prevention System, Deep packet

inspection, URL filtering Antivirus, Bandwidth management, Malware detection. In addition to the older packet filtering and Transmission Control Protocol (TCP) handshakes based firewalls. These can halt threats to the network as well as provide advanced security. NGFW checks the contents of the data and flags possibly harmful data via employing machine learning-based methods or signature-based methods [2]. There has been an inquiry performed to analysis the effectiveness of the NGFW [4] in the Internet of Things (IoT) in an organization and smart home. The firewall is tested with many attacks such as phishing, Distributed Denial of Service (DDoS), also Structure Query Language (SQL) Injection on various networks. NGFW showed enhanced against threats in contrast to other firewall technologies [2]. Traffic categorization techniques via NGFW were used within [5]. This assists in specifying the application-level protocols. Machine learning is employed to specify encrypted traffic. Also, proposed a time-varying Logistic Regression model that is integrated alongside traffic patterns. There is an enhancement in accuracy within this model in contrast to other models. Various machine-learning models can be used to research the data traffic [2]. While Stateful inspection firewall this kind of firewall collects Packet filtering and Circuit-level gateways, as well as TCP handshake to provide better security. This kind is more complicated in contrast to other technologies. A stateful inspection firewall utilizes session tables to keep a flow of the state of connections. The accuracy Stateful inspection firewall is based on the processing of these tables in addition to the packet filtering mechanism [2]. The packet filtering time can be minimized [6] by refusing the packets to be refused by the use of a splay tree firewall. This assists in minimizing time addition to memory space. The timeout data and the session state are classified into many data structures. Within DDoS the data can be contrasted alongside a splay tree additionally can be refused early. Also, excess computational overhead can be escaped [2]. Also, we want to focus on there are different types of network environments like LAN (Local Area Network) and WAN (Wide Area Network). LAN Scope is limited to a small geographic area, for example, a single building. Also, LANs have high data transfer rates because of the utilization of a fast connection and the narrow range the data travels. While it's managing is easier due to its small scope. Other side, WAN connects many LANs to permit resource sharing over long distances as well as communication. Also, it has to reduce data transfer rates in contrast to LANs because of potential variability in connection quality and wide distances. It's more complex to manage due to the need for sophisticated technologies and diverse infrastructure to guarantee reliable communication. The contrast between the Stateful inspection firewall and NGFW is critical for understanding their strengths and limitations in many network environments like LAN and WAN.

The main contribution of this paper is represented as below:

- This study travels deeper into those firewalls executes the practical applications of both firewalls in LAN and WAN environments and checks the performance effects in both of them like accuracy and throughput.
- The result shows that accuracy in Stateful inspection firewall in LAN reaches 54% and the throughput reaches 0.82 packets /ms.
- Stateful inspection firewall in WAN accuracy reaches also 54% and the throughput 1.76 packets /ms.
- NGFW in LAN reaches 60% and the throughput reaches 0.91 packets /ms.
- NGFW in WAN the accuracy reaches 68% and the throughput reaches 0.47 packets /ms.

A network security system is predicted to overcome the challenge of mitigating attacks executed via internal users. Also, this study aims to analyze the effectiveness of the NGFW which is implemented to enhance network security. The method employed in this study is the contrast method with a test of TCP attack, Internet Control Message Protocol (ICMP) smurf attack, User Datagram Protocol (UDP) flood attack, as well as Dynamic Host Configuration Protocol (DHCP) starvation attack on an organization network. The conclusion was that the NGFW enhances the performance for protecting and mitigating attacks executed via internal users on an organization network which means it can increase the security of data communication networks against threats from the internal networks [7]. The weakness of this research is that the attack testing only specific network devices alongside traditional firewall from internal networks and it is suggested that additional study to execute attack testing from the public internet to the internal network to enhance network security. This means this paper executes its work on a LAN network.

Securing applications and networks is an important problem for any scientific corporation. This type of corporation faces security problems, and sensitive information to secure data. So, they use NGFW to enhance security elements to defend applications and networks. The tests were executed over the Atomic Energy Research Establishment (AERE) under the Bangladesh Atomic Energy Commission (BAEC) network zone where Secured

network framework via configuring the NGFW. The structured NGFW at AERE operates on all seven Open System Interconnection (OSI) layers [8]. This configured firewall is used not only for controlling UDP and TCP access, Network Address Translation (NAT), and traffic monitoring connections as layer 4 protocols but also executes on every layer of seven (7) OSI layers. They have executed many applications and network policy rules over the NGFW, and then they have gathered and analyzed statistical network data via NGFW in many network security frameworks. Also, they study the effectiveness of NGFW against many application and network threats. In the future, they will try to analyze data via base on VPN for multilayer firewall, and remote access alongside a network framework. Also, the contrast of performance evaluation of other firewalls like the Stateful inspection firewall depends on different performances like latency, throughput, accuracy, and contrast network security parameters of NGFW and Stateful inspection firewall [8]. This means this paper executes its work on a LAN network.

The attention on detecting escape attacks increases because of weaknesses of the Stateful inspection firewall. These types of attacks enable firewall escape although the rules are configured properly. They proposed implementing and designing a model-guided approach to uncovering similar escape attacks, then they concluded a behavioral model for Stateful inspection firewall development. They depend on TCP protocol in their work. They execute the concluded model to synthesize attack strategies for a given deployment and threat model. Finally, they evaluate their model design on four production-quality firewalls. The results show that analysis of many production-grade firewalls concluded that there are hundreds or a thousand for some cases of clear attack sequences for every Stateful firewall. In addition, these attacks are subtle and would be hard to discover if we had done them manually [9]. In the future, they can consider more complicated attacks like data exfiltration from a Stateful inspection firewall server. Additionally, in this work, they focused on TCP protocol in the future they extend their work using other model interfaces like Hypertext Transfer Protocol (HTTP), GET, and POST [9]. Their paper executes its work on a LAN network.

Their study focuses on hosts that reside in firewalled networks, which is a highly frequent scenario at present. In the implementations of many TCP/IP network stacks, they analyzed the generation of protocol header fields found new methods to leak information about general protocol states, and then illustrated new covert channels via virtual monitoring and editing of the system's global state by these protocol fields. In the exfiltration scenario, their attacks are designed to be non-disruptive which expands their durability and also makes the attacks stealthier assuming similar techniques and alias resolution this guarantees the techniques are ethical. They use different protocols in their work like ICMP, HTTP/3, TCP, and Quick UDP Internet Connections (QUIC). They enabled the development of practical private channels that directly pierce firewalls, otherwise indirectly initiate communication by hosts in firewalled networks that also use Source Address Validation (SAV). They illustrate and test three attacks: exfiltration by the firewall itself, exfiltration by co-resident containers, and exfiltration by a Demilitarized Zone (DMZ) host [10]. These are three general, innovative usage scenarios for private channels that work around firewalling and allow devices that are not permitted direct communication with the Internet. Alternatively, the exfiltration data from isolated networks to the Internet also clarifies how to mount familiar attacks for example container co-residence detection, de-NATting, and host alias resolution utilizing the innovative information leakage techniques [10]. They worked on three general attack scenarios only, but there may be extra attack scenarios exist, which allows future research on this topic. Their paper executes its work on a LAN network.

2. METHOD

The contrast between the Stateful inspection firewall and NGFW is critical for understanding their strengths and limitations in many network environments like LAN and WAN. This study travels deeper into those firewalls executes the practical applications of both firewalls in LAN and WAN environments and checks the performance effects in both of them like accuracy and throughput.

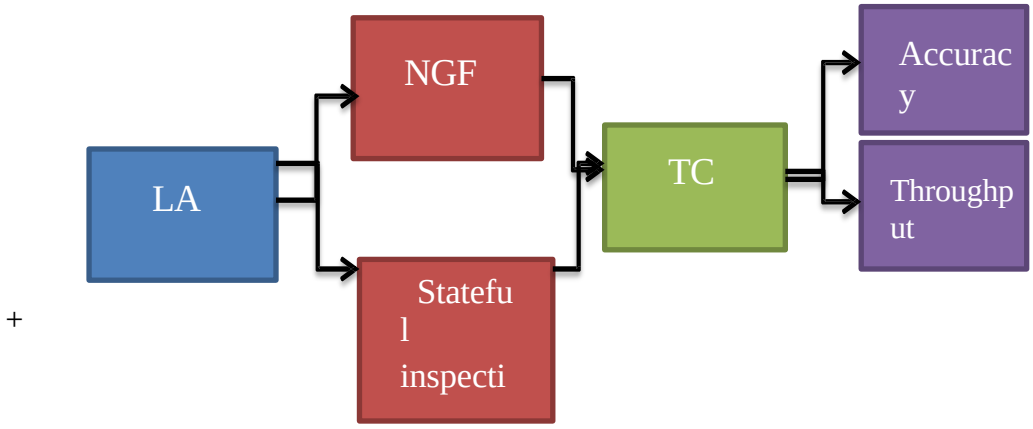

Figure 1. NGFW and Stateful inspection firewall in LAN environment.

Our work contains two parts, the first part executes our work in a LAN environment, as shown in Figure 1. Next-generation firewall execute in a LAN environment and test by sending attacks using TCP packets from the clients to the server. The test performance is based on accuracy, which refers to the degree to which data transmitted among a network is received without alterations or errors. Also, test performance is based on throughput, which refers to the rate at which data is successfully transmitted from the source to the destination in a given period, and reflects the real data transfer rate, considering factors for example protocol overhead, network congestion, and any retransmissions. It indicates the capacity and efficiency of a network to stop data traffic.

While second part executes our work in the WAN environment, as shown in Figure 2. The same proposed accuracy and throughput.

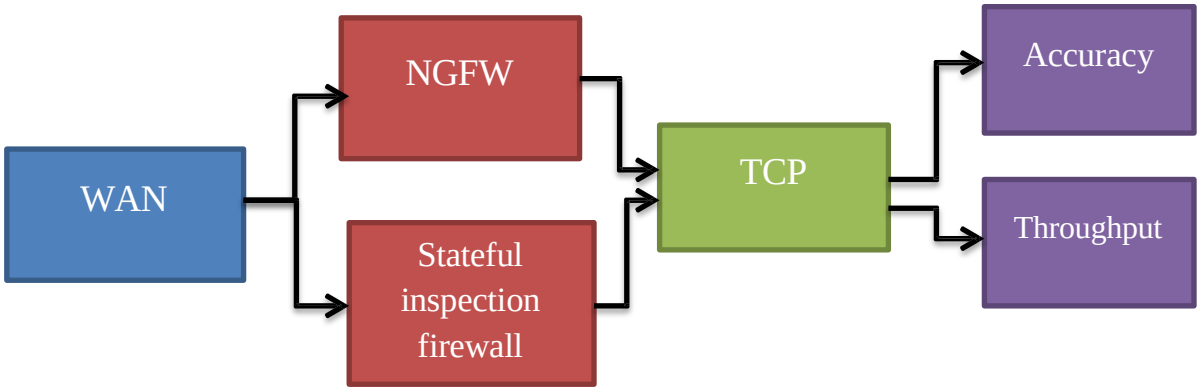

Figure 2. NGFW and Stateful inspection firewall in WAN environment.

work of LAN is executed in the WAN environment. We also test the NGFW and Stateful inspection firewall by sending attacks using TCP packets from the clients to the server. Moreover, the test performance is based on The main chart of our work is shown in Figure 3.

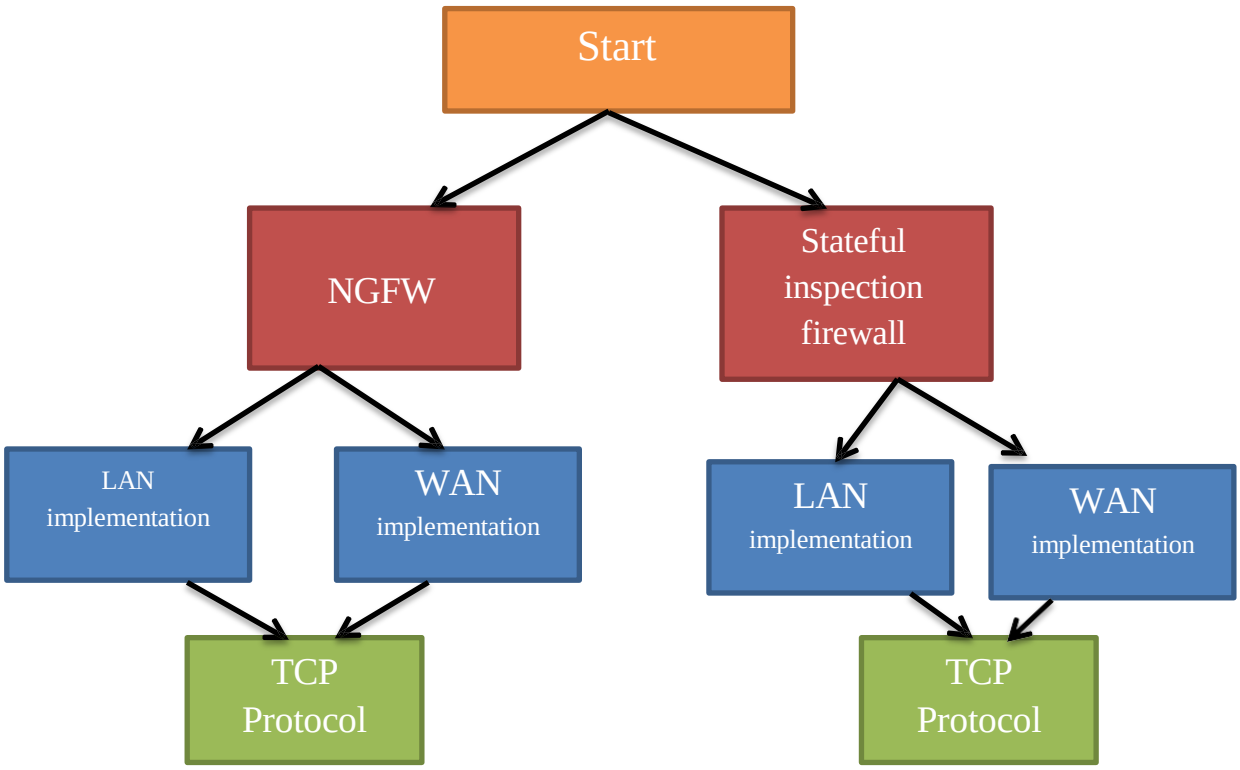

Figure.3. The main chart of both firewalls in LAN and WAN environments

3. RESULTS AND DISCUSSION

In our work, we depend on the eclipse-java-2023 program and use Java language. In Figure 4 you can see that the general topology of this paper is sending 50 TCP packets from the client to the server one time using NGFW in LAN and WAN environment, and another time sending 50 TCP packets from the client to the server using Stateful inspection firewall in LAN and WAN environment. The performance evaluation depends on accuracy and throughput.

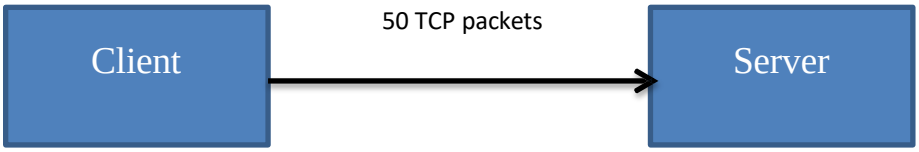

Figure 4. The general topology of this paper.

Table 1. Paper results on Local Area Network.

Firewall type	Accuracy	Throughput
NGFW	68%	0.89 packets/ms
Stateful inspection firewall	54%	0.83 packets/ms

On LAN, depends on Table.1 we send 50 TCP packets from the client to the server using NGFW and gain an accuracy rate of 68% and throughput of 0.89 packets/ms. Also, we send 50 TCP packets from the client to the server using a Stateful inspection firewall and gain an accuracy rate of 54% and throughput of 0.83 packets/ms, which depends on the results NGFW much better than Stateful inspection firewall in LAN environment, as shown in Figure.5.

++

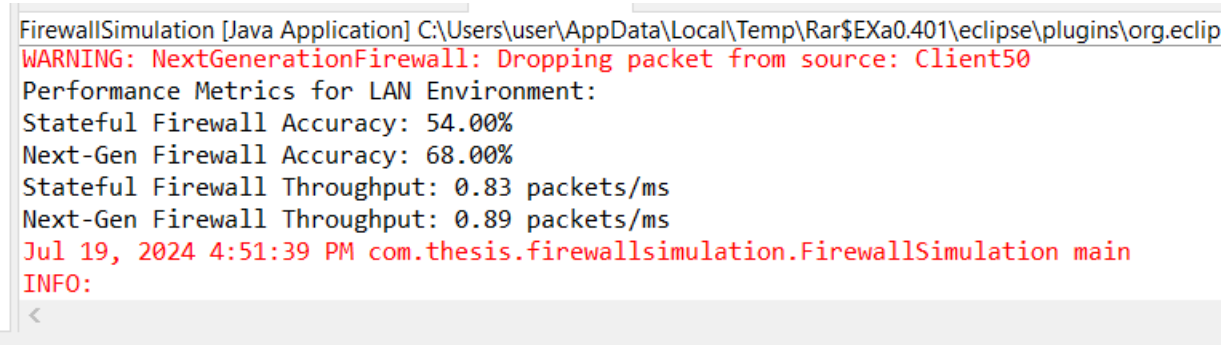

Figure 5. Results on Local Area Network.

On WAN, depends on Table.2 we send 50 TCP packets from the client to the server using NGFW and gain an accuracy rate of 56% and throughput of 0.44 packets/ms. Also, we sent 50 TCP packets from the client to the server using the Stateful inspection firewall and gained an accuracy rate of 48% and throughput of 1.57 packets/ms, which depends on the results NGFW better than Stateful inspection firewall when using accuracy as performance, while when using throughput Stateful inspection firewall better than NGFW, as shown in Figure.6.

Table 2. Paper results on Wide Area Network.

Firewall type	**Accuracy**	**Throughput**
NGFW	56%	0.44 packets/ms
Stateful inspection firewall	48%	1.57 packets/ms

```
<terminated> FirewallSimulation [Java Application] C:\Users\user\AppData\Local\Temp\Rar$EXa0.171\ecli
INFO: NextGenerationFirewall: Forwarding packet to destination: Server8
Performance Metrics for WAN Environment:
Stateful Firewall Accuracy: 48.00%
Next-Gen Firewall Accuracy: 56.00%
Stateful Firewall Throughput: 1.57 packets/ms
Next-Gen Firewall Throughput: 0.44 packets/ms
```

Figure 6. Results on Wide Area Network.

4. CONCLUSION

Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology, combining a conventional firewall with other network device filtering functions, such as an application firewall using in-line Deep Packet Inspection (DPI), an intrusion prevention system (IPS). Stateful inspection firewall also referred to as Stateful packet inspection is a network-based firewall that individually tracks sessions of network connections traversing it, and it operates by monitoring active connections making decisions based on the state of the traffic. Firewall weakness in several types of networks caused negative effects and dropped down the network and broke over privacy. We create a scenario based on TCP protocol to evaluate the efficiency of the firewall based on two main measurement elements that represent accuracy and throughput. Also, this paper provides a comparative analysis of Stateful inspection firewalls and Next Generation Firewalls (NGFWs) within Wide Area Network (WAN) Local Area Network (LAN) environments. In our work, we depend on the eclipse-java-2023 program and use Java language. The results in LAN show that NGFW is much better than the Stateful inspection firewall which gains an accuracy of 68% and throughput of 0.89 packets/ms, in WAN NGFW i s better than the Stateful inspection firewall when using accuracy reaching 56% as performance but when using throughput Stateful inspection firewall better than NGFW reach 1.57 packets/ms. Our future work depends on increasing the rate of accuracy and throughput in Stateful inspection firewalls.

ACKNOWLEDGEMENTS

Author thanks ... . In most cases, sponsor and financial support acknowledgments.

REFERENCES

[1] Sina Ahmadi; Next Generation AI-Based Firewalls: A Comparative Study; International Journal of Computer (IJC); 2023; No.49; Issue 1; ISSN 2307-4523; pp.245-262.

[2] Padma Priya Mukkamala, Sindhu Rajendran; A SURVEY ON THE DIFFERENT FIREWALL TECHNOLOGIES; International Journal of Engineering Applied Sciences and Technology (IJEAST); 2020; Vol. 5; Issue 1; ISSN No. 2455-2143; Pages 363-365.

[3] Vinay T. Patil, Purushottam R. Patil , Vinayak O. Patil, Shweta V. Patil; Performance and information security evolution with firewalls; International Science and Technology Journal; 2018; Vol. 7; Issue 2; ISSN NO: 1632-2882.

[4] Benfano Soewito, Charlie Erwin Andhika; Next Generation Firewall for Improving Security in Company and IoT Network ;International Seminar on Intelligent Technology and Its Applications (ISITIA); 2019; Surabaya, Indonesia.

[5] Yiyang Shao, Luoshi Zhang, Xiaoxian Chen, Yibo Xue; Towards time-varying classification based on traffic pattern; IEEE Conference on Communications and Network Security; 2014; San Francisco, CA, USA.

[6] ZOUHEIR TRABELSI, SAFAA ZEIDAN, KHALED SHUAIB, AND KHALED SALAH; Improved Session Table Architecture for Denial of Stateful Firewall Attacks; IEEE Access; 2018; Vol. 6.
[7] Nico Surantha; Evaluation of Data Center Network Security based on Next-Generation Firewall; International Journal of Advanced Computer Science and Applications (IJACSA); 2021; Vol. 12; No. 9.
[8] Md. Shamimul Islam , Mohammed Asraf Uddin, Dr. Md. Dulal Hossain, Dr. Md. Shakil Ahmed and Dr. Md. Golam Moazzam; Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall; International Journal of Computing and Digital Systems; 2023; ISSN (2210-142X), No.1.
[9] Soo-Jin Moon, Yves Bieri, Ruben Martins, Vyas Sekar; Automatic Discovery of Evasion Attacks Against Stateful Firewalls; Carnegie Mellon University; 2021.

BIOGRAPHIES OF AUTHORS (10 PT)

The recommended number of authors is at least 2. One of them as a corresponding author.
Please attach clear photo (3x4 cm) and vita. Example of biographies of authors:

	**Asst. Lecturer. Sally A. Al-Hasnawi**, Received Here Msc. degree in the Networks engineering from University of Al-Nahrain, Baghdad – Iraq in 2017. She has been a full-time lecturer in Al-Nahrain University College of information engineering cybersecurity department, Baghdad, Iraq, since March 2023. She can be contacted at email: sally.a.karim@nahrainuniv.edu.iq
2 Author 2 picture	**Dr. Aws A. Abdulsahib**, Received His PhD. degree in the Information and communication technology from University of UNITEN, Kuala Lumpur – Malaysia in 2022. Department of Computer Science, University of Dijlah, Baghdad, Iraq , Email: aws.kareem@duc.edu.iq