Proceedings of to the 9th Scientific Conference of University of Garmian: Pure science and Technology Applications (SCUG-PSTA-2022). Kalar (46021) / Sulaymaniyah (26-27 Oct.2022) (Special issue for Passer journal of basic and applied sciences) Paper No. 04, 51-62

Multi-layered firewall to mitigate the impact of Distributed Denial of Service on a network

Dana Hasan Ahmed[1]*, Rebeen Rebwar HamaAmin[2]

[1*] Computer Science Department, College of Science, University of Garmian, Kalar, Sulaymaniyah, Iraq

[2] Network Department, Computer Sciences institute, Sulaimani Polytechnic University, Sulaymaniyah, Iraq
dana.hasan@garmian.edu.krd ; rebeen.rebwar@spu.edu.iq

ABSTRACT

A firewall is one of the key components in securing an organization's network and computational assets against different network and application-based attacks. Most firewall solutions only consider one or two layers of TCP/IP networking architecture to protect against attacks, especially spoofing-based attacks. In contrast, there are some proposed solutions to protect against such attacks. However, these solutions work in areas such as clouds or Software Defined Networks (SDN), and legacy networks cannot utilize such techniques. Therefore, establishing a type of firewall that can be scalable, strong, and easy to implement is a challenge necessary for a new firewall technique to prevail. This paper presents a novel strategy to implement a multi-layered firewall to overcome the current state-of-art firewalls. Our firewall combines a packet-filtering approach (i.e., Internet and Transport layer) with an application layer firewall under the umbrella of Stateful-Packet-Inspection. The experiments were performed in a controlled environment with 1% legitimate packets, and 99% spoofed traffic on average. The Stateful-Packet-Inspection discards any packets based on their traffic flow given to them by the firewall while informing the network administrator about the system breach passively. The results of the experiments are benchmarked with previous works and showed improvement in accuracy by 13.5% and sensitivity by 13.75% while decreasing the false negative rate by 86.5% with minimal computational and network overhead.

KEYWORDS: Firewall, Distributed Denial of Services, TCP/IP architecture, Spoofing, traffic signature

1 INTRODUCTION

Computer networks are groups of computing devices connected through a medium that facilitate information and resource sharing. Unfortunately, it also creates opportunities for cybercriminals to try to gain unauthorized access to any assets (i.e., computers, data, and information) crucial to an organization [1]. The exponential growth of security risks and dangers that exists outside of a network in the present times can strictly confirm the necessity for people to use and study different methods to prevent Distributed Denial of Service (DDoS). Several techniques to avoid or mitigate spoofing-based attacks, such as firewalls and Virtual Private Networks (VPN), protect computational resources from getting damaged, especially during high-volume flooding attacks [2]. A firewall is a hardware, software, or hybrid-based security mechanism that monitors and controls the flow of traffic between a trusted network and outside of it[3][4].

Firewalls filter outgoing and incoming packets to/from a computer or network, using filtering rules that reflect and enforce the organization's security policy. The firewall inspects all packets entering or leaving a computer or a network and then decides on every packet that crosses it; each packet is either allowed or denied passing the firewall [5]. However, more sophisticated attack techniques allow attackers to monitor a network, getting the network's traffic signature. Therefore, designing a new type of firewall that can protect networks from spoofed traffic is essential. The most suitable solution is developing a new technique to take advantage of the Internet, Transport, and Application layer is vital to prevent the attackers from mimicking the network traffic, thus attacking their targeted system [4][5].

In this paper, we implemented a firewall technique in the Application, Transport, and Internet layers of the TCP/IP model. First, we describe different firewall techniques in different computational and networking environments (i.e., Software Defined Networking (SDN) and VPN). Then, we benchmark the proposed scheme with another competitive work, and the results are discussed in detail. Then, we show how this work can help prevent flooding attacks with complex traffic signatures with little resource overhead. The rest of the paper is organized as follows: Section 2 reviews different Firewall techniques in different computational and networking environments. Section 3 shows information about previous works related to the topic of this paper. Section 4 illustrates the implementation of the proposed approach. Section 5 presents the work's outcome and discusses the results giving proper discussion about the results. Finally, section 6 concludes the article and offers future works related to the study.

2 TYPES OF FIREWALLS

Firewalls are an essential building block of network security in any organization and can be divided into two primary types, a Host-based firewall, and a Network-based firewall. The Host-based firewalls filter the traffic from/to hosts or end devices. In contrast, Network-based firewalls help to secure connections

between networks and network devices. Legacy firewalls implemented static, pre-installed rules such as access policy lists to control the network traffic. However, due to the ever-complexity-increasing attacks, the firewalls have evolved to spot and respond to any threats dynamically. The different types of Firewall technologies work at different layers of the TCP/IP model [6][7].

2.1 Packet filtering

It is the simplest and oldest kind of firewall configured to work with a set of installed rules that take the source Internet Protocol (IP), destination IP, port number, and other information. The packet cannot pass the firewall unless it matches the installed rules. Then, the packet is dropped, and an ICMP packet informs the packet's source or is discarded silently. This type of firewall is straightforward to implement. However, the weakness of this kind of firewall is that it may suffer from conflicting rules which leads to vulnerability [8].

2.2 Circuit-level gateway

Circuit-level gateway is a basic firewall that does not require too much overhead. It works based on Transmission Control Protocol (TCP) handshake to allow or deny traffic. That is why preventing incoming malware from entering a system is not the best solution. However, it can be utilized in certain situations [9].

2.3 Stateful packet inspection

A stateful packet inspection firewall combines packet filtering and TCP handshake to provide better security. It is a complex technology that causes performance degradation when it operates at the cost of security. It works based on a session table to keep stores the state of connections. These firewalls can work to best avoid Denial of Service (DoS) attacks by working with the session tables inside them [4][10].

2.4 Proxy firewalls

This type of firewall works at the network edges by filtering the traffic between the source and the network at the application layer of the TCP/IP model. The content of network packets is inspected by establishing a connection between the proxy firewall and the packet source. The proxy firewall also examines the packet for any existing malware and the TCP handshake protocol. The data is granted permission to leave to the destination only when it can pass the rules of the proxy firewall [11].

2.5 Next generation

This type of firewall protects networks by combining multiple layers of protection such as Intrusion Prevention Systems (IPS), Antivirus, URL filtering, Malware detection, bandwidth management, rate limiting, and more, with TCP handshake firewalls and traditional packet filtering firewalls. However, such techniques can dramatically escalate a system's security level 12].

2.6 Cloud firewall

Traditional firewalls cannot protect cloud data centers. Therefore, it is essential to have a technology that can detect anomalies within cloud data centers. Dynamic resource allocation and event detection is used to establish a framework. Since SDN offers centralized network management, which allows for network programmability. SDN stands out as a new networking paradigm that can give protection to resources any corporation or service provider uses to secure their assets. The cloud firewall can protect against the application layer and other forms of attacks [9].

3 RELATED WORKS

In [1], the authors analyzed the impact of securing IoT in a smart house and a company network by implementing a Next Generation firewall. They attacked the system with DDoS attacks, SQL injection, and phishing attacks on the company network and the smart house. The results of their experience showed the significance of using a Next Generation firewall in providing better protection performance for the smart house and the company network from different threats from the Internet

In [4], the authors presented a distributed-based firewall to counter reflection/amplification attacks, a form of Distributed Denial of Service (DDoS) attacks. Their method showed a 19.9% improvement in CPU load during attacks. Their defense mechanism showed to protect upstream networks to the target from exhaustion due to the sheer volume of attack traffic by eliminating spoofed packets from getting any responses from authoritative DNS servers

In [11], the authors proposed and demonstrated a Web Application Firewall (WAF) using ModSecurity and the Reverse proxy method on a web-based application. From the tests they held on to SQL injection, unauthorized vulnerability Web-scanning and cross-site scripting attacks were detected and countered by WAF when used with ModSecurity and Reverse proxy method.

4 MULTI-LAYERED FIREWALL

The system model was implemented to install the proposed solution on two physical machines. Each physical machine used a VMware workstation to create two virtual machines to replicate each device. The figure below shows how the system components are logically connected.

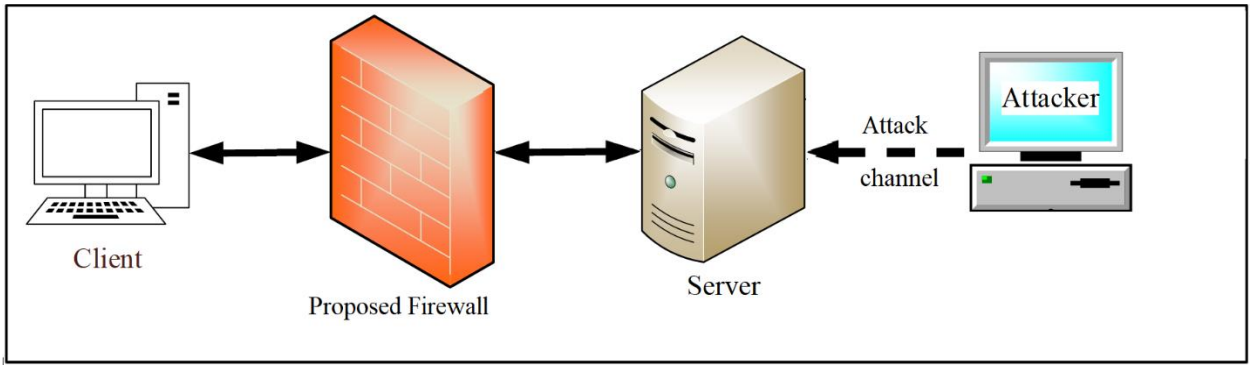


Figure 1: Logical design of the system model

The proposed firewall is implemented using Java programming language, and the information about session tables is stored in a MySQL table. The anomaly in spoofed packets is a mismatch in the source port, destination port, and the requested service. Therefore, we can design and build our firewall strategy based on this fruitful idea. In this work, the client sends requests through the firewall to the server asking for a service. When the firewall receives the request packet through its listener, it stores information about the packet in its table. The information regarding the packet consists of source IP address, destination IP address, source port, destination port, and service type (i.e., monlist for NTP, TXT for DNS, and more), as shown in figure 2. Then it sends the request to the server.

At the same time, the attacker tries to flood the client with bogus traffic using spoofing traffic with the client's IP address. The server responds to every incoming request (client and attacker requests) and sends back the traffic to the client. The firewall receives the requests and starts comparing them with its table. If there is a mapping between the server's response and the firewall table, the response is allowed and sent back to the client. Figure 3 shows the proposed firewall diagram in detail.

If no mapping occurs, the firewall discards the response and creates a log record to inform the network administrator about the incident. Moreover, suppose a request inside the firewall table did not get any response in a pre-defined time slice. In that case, the table automatically discards it to prevent the table size from overgrowing.

source_ip	des_ip	source_port	des_port	service_type	C_result
192.168.1.1	192.168.1.100	65533	53	TXT	unsuccessfull
192.168.1.1	192.168.1.100	65533	53	NXT	unsuccessfull
192.168.1.1	192.168.1.100	65533	53	PTR	successfull
192.168.1.1	192.168.1.100	65533	53	A	unsuccessfull
192.168.1.1	192.168.1.100	65533	53	*	unsuccessfull
192.168.1.1	192.168.1.100	65533	53	SOA	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	CNAME	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	MX	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	NS	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	TXT	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	NXT	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	PTR	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	A	unsuccessfull
192.168.1.1	192.168.1.100	65530	53	*	unsuccessfull

Figure 2: Firewall table snapshot

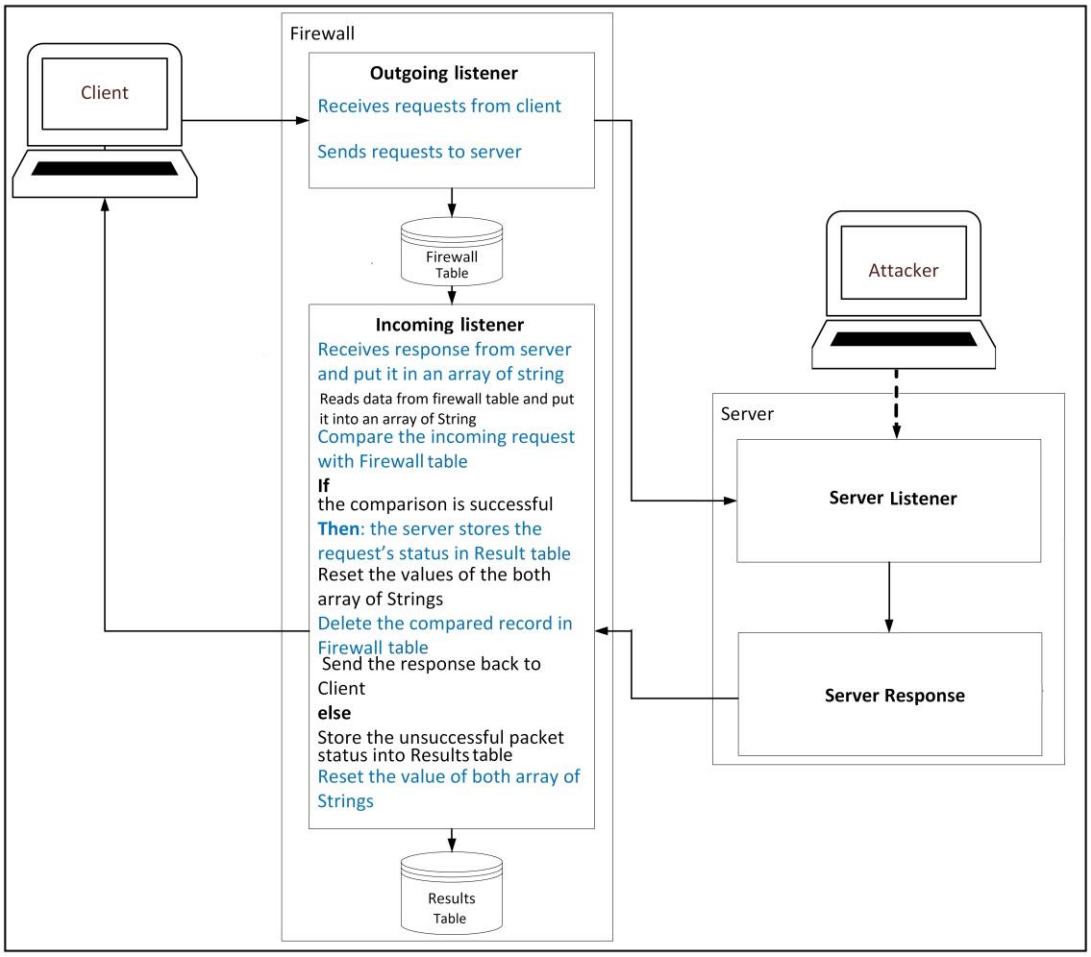


Figure 3: Diagram of the proposed work

4.1 Performance metrics

The definition of performance metrics can be based on predictions or decisions which a defense mechanism makes. For example, defense mechanisms may detect and respond to or bypass the attack [13]. There are four possible outcomes based on the defense mechanism's response shown in table 1.

Table 1 Defense mechanism outcomes and desirable outcomes [13]

		The desirable decision of the defense mechanism	
		Negative	Positive
Defense decision	Negative	True Negative (TN)	False Negative (FN)
	Positive	False Positive (FP)	True Positive (TP)

The first outcome is called True Negative (TN) because both the desired and defense mechanism results are negative. The second outcome is False Negative (FN) since the desired outcome is positive and the defense mechanism's outcome is negative. Finally, the desired outcome was negative, and the defense mechanism's outcome was positive. Therefore, the third outcome is called False Positive (FP). Finally, the outcome is called True Positive if both the desired and defense mechanism results are positive. Therefore, according to [13], these outcomes can be utilized to evaluate a defense mechanism's strength: Accuracy, Sensitivity, and False Negative Rate.

Accuracy (ACC) is the ratio of the correct outcomes of the defense mechanism (TN, TP) over the total outcomes of the defense mechanism (TN, FN, FP, TP). Equation (a) measures the accuracy of a defense mechanism.

$$Acc = \frac{(TN + TP)}{(\mathrm{TN} + \mathrm{FN} + \mathrm{FP} + \mathrm{TP})} \dots\dots (a)$$

Sensitivity (Sen) is the ratio of true positives (TP) over total positive outcomes (TP+FN). Equation (b) measures the sensitivity of a defense mechanism

$$Sen = \frac{(TP)}{(TP + FN)} \dots\dots (b)$$

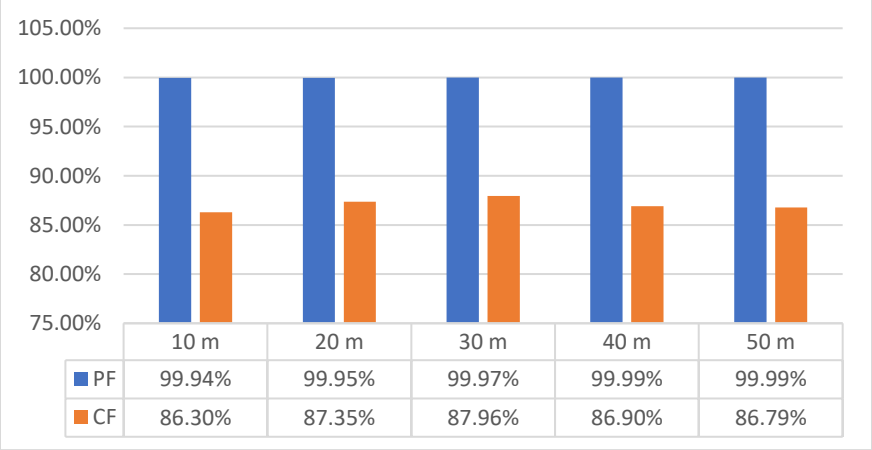
False-negative rate (Fnr) is the ratio of false-negative outcomes (FN) of the defense mechanism over total negative outcomes of the defense mechanism (TN+FN). Equation (c) measures the false-negative rate of a defense mechanism

$$Fnr = \frac{(FN)}{(TN + FN)} \dots\dots (c)$$

5 RESULTS AND DISCUSSION

The output of the experiments shows the significance of the Proposed Firewall (PF) in mitigating the impact of flooding attacks on the client with minimal overhead. The results are benchmarked with the Competitive Firewall (CF) [14] in the same computational environment and same input volume and setting. The experiments run in five replications with different attack duration. The traffic volume is orchestrated, so it only contains 1% legitimate packets; the rest is attack packets sent by the attacker toward the client. The performance metric which is considered is defense strength. Figure 4 shows the defense strength outcomes.

As the figure shows, the proposed firewall shows an increased ability to differentiate between spoofed and legitimate traffic because the proposed firewall uses all information regarding any packets, such as IP address, port number, and service types. We can illustrate the detection accuracy based on the outcome provided by the firewall table based on equation (a). Figure 4 shows the detection accuracy.



	10 m	20 m	30 m	40 m	50 m
PF	99.94%	99.95%	99.97%	99.99%	99.99%
CF	86.30%	87.35%	87.96%	86.90%	86.79%

Figure 1: Detection accuracy

Calculating sensitivity requires us to put the outcome of the firewall table according to equation (b). as shown in figure 5.

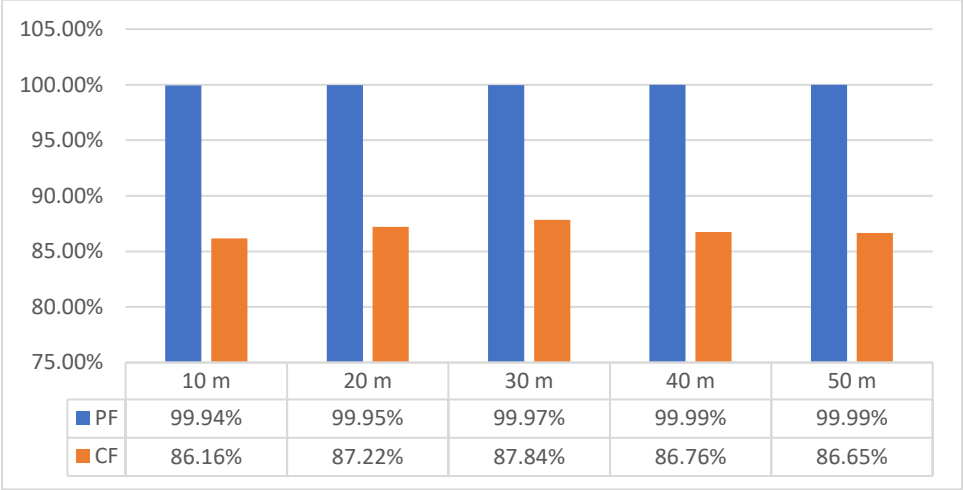


Figure 5: Detection sensitivity

Finally, to measure the false negative rate of both the proposed and competitive firewall, equation (c) is used, as shown in figure 6.

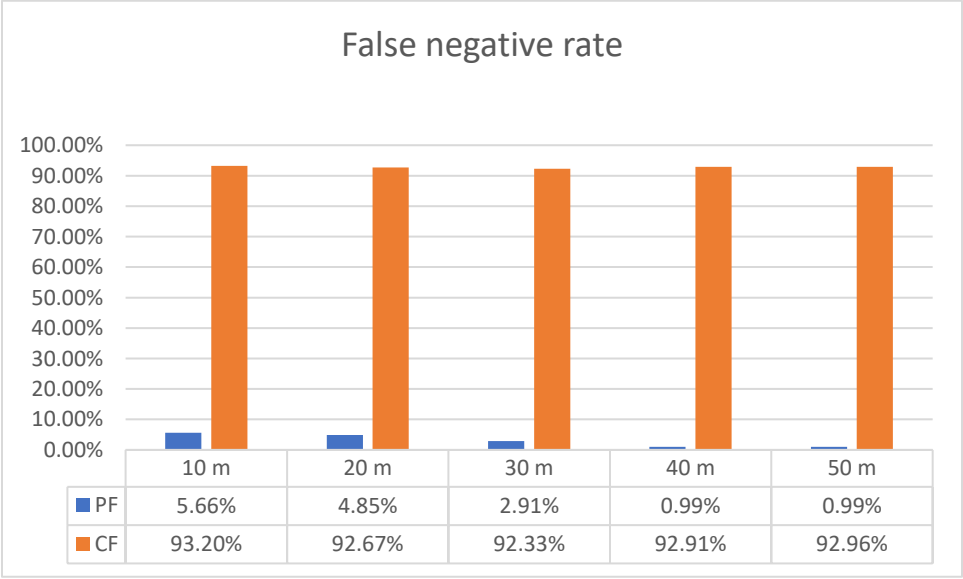


Figure 6: False negative rate

As the results show, with an increase in attack duration, the defense strength increases, giving fewer false outcomes, thus improving the accuracy, sensitivity, and false negative rate results. The massive difference between PF and CF is that the total percentage of legitimate packets is 1% which increases the false negative rate for the CF firewall.

6 CONCLUSION

Availability is one of the critical features of any information system and its users. However, attacks such as DDoS can significantly disrupt the availability of services provided by an information system. This work presented a multi-layered firewall to counter spoofing-based attacks, usually used to launch DDoS attacks. Instead of using one or two layers of TCP/IP architecture, we used the top-three layers of the mentioned network architecture to differentiate legitimate traffic from spoofed ones. The results showed around a 13.6% improvement in accuracy compared to competitive work.

On top of that, we showed that our system could show better sensitivity to attack traffic, up to 13.75%. Furthermore, the experiments showed that the proposed method decreases the false negative outcomes by 86.5% for the network traffic. The increase in defense strength comes with minimal overhead on the firewall and other system components.

REFERENCES

1. B. Soewito and C. E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," Proceedings - 2019 International Seminar on Intelligent Technology and Its Application, ISITIA 2019, pp. 205–209, Aug. 2019, DOI: 10.1109/ISITIA.2019.8937145.
2. S. Jingyao, S. Chandel, Y. Yunnan, Z. Jingji, and Z. Zhipeng, "Securing a Network: How Effective Using Firewalls and VPNs Are? " 2020, pp. 1050–1068. DOI: 10.1007/978-3-030-12385-7_71.
3. G. Dayanandam, T. v. Rao, D. Bujji Babu, and S. Nalini Durga, "DDoS Attacks—Analysis and Prevention," 2019, pp. 1–10. DOI: 10.1007/978-981-10-8201-6_1.
4. R. R. Hama Amin, D. Hassan, and M. Hussin, "Preventing DNS Misuse for Reflection / Amplification Attacks With Minimal Computational Overhead on the Internet,"

Kurdistan Journal of Applied Research, pp. 60–70, Dec. 2020, DOI: 10.24017/science.2020.2.6.

5. Z. Trabelsi and H. Saleous, "Exploring the Opportunities of Cisco Packet Tracer For Hands-on Security Courses on Firewalls," in 2019 IEEE Global Engineering Education Conference (EDUCON), Apr. 2019, pp. 411–418. DOI: 10.1109/EDUCON.2019.8725112.
6. M. J. Awan et al., "Real-Time DDoS Attack Detection System Using Big Data Approach," Sustainability, vol. 13, no. 19, p. 10743, Sep. 2021, DOI: 10.3390/su131910743.
7. P. P. Mukkamala and S. Rajendran, "A SURVEY ON THE DIFFERENT FIREWALL TECHNOLOGIES," International Journal of Engineering Applied Sciences and Technology, vol. 5, no. 1, pp. 363–365, May 2020, DOI: 10.33564/IJEAST.2020.v05i01.059.
8. J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2022, pp. 0752–0759. DOI: 10.1109/CCWC54503.2022.9720435.
9. Y. Gautam, K. Sato, B. P. Gautam, and N. Shiratori, "Novel Firewall Application for Mitigating Flooding Attacks on an SDN Network," in 2021 International Conference on Networking and Network Applications (NaNA), Oct. 2021, pp. 449–455. DOI: 10.1109/NaNA53684.2021.00084.
10. D. Hasan, R. R. Hama Amin, and M. Hussin, "Efficient Authentication Mechanism for Defending Against Reflection-Based Attacks on Domain Name System," Kurdistan Journal of Applied Research, vol. 5, no. 1, pp. 164–174, Jun. 2020, DOI: 10.24017/science.2020.1.12.
11. R. A. Muzaki, O. C. Briliyant, M. A. Hasditama, and H. Ritchi, "Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall," in 2020 International Workshop on Big Data and Information Security (IWBIS), Oct. 2020, pp. 85–90. DOI: 10.1109/IWBIS50925.2020.9255601.

12. K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security: A Survey," Conference Proceedings - IEEE SOUTHEASTCON, vol. 2018-April, Oct. 2018, DOI: 10.1109/SECON.2018.8478973.
13. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013, DOI: 10.1109/SURV.2013.031413.00127.
14. M. H. and A. A. Dana Hasan, "Effective Amplification Mitigation and Spoofing Detection During DNS Flooding Attacks on Internet.," Journal of Engineering and Applied Sciences, 12: 475-480., vol. 12, no. 3, pp. 475–480, 2017.