

# Implementation of Multihomed Firewall Based on IDS and DMZ Technology Using PfSense

Roki Hendrawan<sup>1\*</sup>, Lilik Widyawati<sup>2</sup>, Ondi Asroni<sup>3</sup>, Husain<sup>4</sup>, Muhamad Wisnu Alfiansyah<sup>5</sup>

<sup>1,2,3,4,5</sup>Fakultas Teknik, Universitas Bumigora  
[rokihendrawan07@gmail.com](mailto:rokihendrawan07@gmail.com) <sup>1\*</sup>

---

## Abstract

As cyberattacks increase, it is necessary to strengthen the mechanism of network defense. Ancae, it is necessary to improve cos This research aims to design and implement a multihomed firewall system using pfSense enhanced with Demilitarized Zone (DMZ) and Intrusion Detection System (IDS) Suricata to strengthen network security. This research uses a simulation-based experimental method in a virtualized environment, using VMware with three main network segments: WAN, LAN, and DMZ. Firewall rules are configured to segment traffic and enforce strict access control, while Suricata is integrated with the Emerging Threats Open (ET Open) ruleset to detect known attack patterns in real-time. Various attack pattern scenarios, including DoS, port scanning, and common brute force, were used to test the system. Log analysis showed that the firewall successfully blocked unauthorized access attempts and effectively segmented the network, while the IDS generated accurate alerts with minimal false positives. These results confirm that integrating pfSense, DMZ, and Suricata IDS provides a complex and responsive network defense strategy suitable for academic and medium-sized enterprise environments.

**Keywords:** Network Security, Multihomed Firewall, Pfsense, IDS, DMZ.

---

## 1. Introduction

Computer network security is an important aspect in ensuring the sustainability of digital services in the midst of rapid technological transformation. It involves a set of procedures and protocols designed to maintain the integrity, confidentiality, and availability of data transmitted over a network[1]. As connectivity increases and network-connected devices grow, threats to information system security also grow more complex, structured, and coordinated. Attacks on networks have gradually shown large-scale, coordinated, and multi-stage characteristics in recent years[2]. According to a recent report from Cloudflare, in the fourth quarter of 2024, their autonomous DDoS defense system successfully detected and blocked various attacks, such as DDoS attacks with peaks reaching 5.6 terabits per second, which is the largest attack recorded to date[3]. So it is necessary to have adequate preventive and protective measures implemented in the network system. Therefore, the management of network security systems needs to be taken seriously to prevent leakage of important information[4]. Computer network security protection not only includes vulnerability detection, encryption, and securing information and networks but is also very important in maintaining privacy and protecting internal resources[5]. By dividing the network into internal and external networks, it can manage data security on the internal network and strictly limit unauthorized access[6].

PfSense is one of the open-source FreeBSD-based firewall platforms[7]. With the development of network communications, multihome technology emerged that handles more than one network path[8]. One of the features in pfSense offers multihome capabilities, as well as the ability to improve security and network traffic management, allowing network connectivity over more than one interface path[9], namely WAN, LAN, and DMZ. All three provide great flexibility in network traffic management and security segmentation, plus pfSense has several features that can be integrated to effectively enhance network security[10]. In the traditional sense, the use of firewalls to defend against intrusion is a more recommended network security operation[11]. Intrusion Detection System (IDS) is a system that monitors whether network traffic is normal or malicious[12]. IDS are designed to examine traffic passing through a network and use predefined rules or known malicious patterns to label the data[13]. A signature-based IDS will detect previously known threat patterns to minimize the occurrence of false positives so that the system produces true positives from the warnings given by the intrusion detection system. The IDS will monitor network traffic that passes through an interface. False negative results have a significant impact because they have a risk of targeting the actual environment, but the system cannot identify it[14]. Meanwhile, the demilitarized zone (DMZ) acts as an intermediate zone designed for additional security on computer networks by separating publicly accessible services (such as web servers and so on) from more sensitive internal networks[15]. The DMZ mechanism is designed to protect internal systems by applying filters that block access to the system to unauthorized entities[16].

The main problem that is the focus of this research is how to implement a multihome firewall system based on Demilitarized Zone (DMZ) technology and Intrusion Detection System (IDS) using pfSense to improve network security. In addition, how the integration between DMZ and IDS can provide optimal protection against attacks from outside and inside the network. Cyberattack protection strategies are based on the assumption that attackers will randomly select networks as targets. If a network has strong defense capabilities, attackers tend

to retreat and switch to other targets that have weaker security levels[17]. Research in the field of cybersecurity is becoming increasingly important as the use of networks in modern life increases[18].

Network security is not just a complementary need but has become a core component in the design and implementation of modern information systems. Organizations that ignore the security aspect risk losing data, reputation, and even critical assets. This research designs and implements a network architecture that combines pfSense multihome firewall, Suricata-based IDS, and DMZ as an isolation zone. Simulations were conducted in a virtual environment with a topology that represents modern network infrastructure to observe the effectiveness of threat detection and network segmentation. The concept of network security has evolved from static firewalls to the integration of multiple security components. This research adopts the latest approach by using the latest version of pfSense, multihome technology, as well as signature-based IDS, which has been proven effective in detecting known attack patterns. It also enables efficient management of traffic between segments.

## 2. Research Method

This research is experimental research with a simulation-based method. The experimental approach was chosen because it allows researchers to observe the effects of implementing a multihome firewall-based network security system, Demilitarized Zone (DMZ), and Intrusion Detection (IDS) using Suricata in a controlled virtual environment[19]. Simulation methods are conducted to test the effectiveness of the system in detecting and counteracting various cyber threats, such as DoS attacks, port scanning, and brute force attacks. This method is relevant because it is able to mimic real situations without disrupting the physical network infrastructure. The simulation method is adopted from the simulation model of testing network security systems in a virtual environment as described by previous research[20]. Adjustments were made by adding IDS-based test scenarios using Suricata as well as adjusting the multihome structure in pfSense to reflect actual network conditions. In addition, the integration of Suricata with the signature database from ETOpen was carried out as an effort to update the detection of more accurate and up-to-date attack patterns. The procedural stages of this research consist of

1. Network Topology Design: Design a virtual network architecture consisting of three main interfaces, namely WAN, LAN, and DMZ.
2. System Implementation: This stage installs and configures devices on the network system, including pfSense, such as creating firewall rules and configuring Suricata as an IDS.
3. System Testing: Testing network services and simulating attacks such as DoS (hping3), nmap scanning, and brute force using hydra to observe the reaction of the system.
4. Log Collection: Retrieve logs from pfSense and Suricata firewalls during simulated attacks.
5. Analysis: Analyze the system's ability to detect and mitigate attacks with descriptive qualitative analysis methods based on the results of system logs and notifications.

The logs collected in this study were obtained directly from the simulation results of the network security system implementation, including network activity logs as well as warning notifications from the IDS system. The source of the logs comes from observing the virtual network system built using VMware Workstation, as well as the configuration results of the pfSense- and Suricata-based systems. The analysis was done qualitatively with a descriptive approach. The set of logs is analyzed based on direct observation of the system response when an attack occurs. Indicators analyzed include alert logs from the Suricata IDS, traffic blocking status on the firewall, number and type of attacks detected, and system response time to attacks. The system logs were used to evaluate the effectiveness of the security system implementation, as well as to provide recommendations for the development of similar network security technologies in the future.

### 2.1. Network Topology Design

In the topology design stage for network security system architecture, it is carried out by considering the needs and functions of each interface and device.

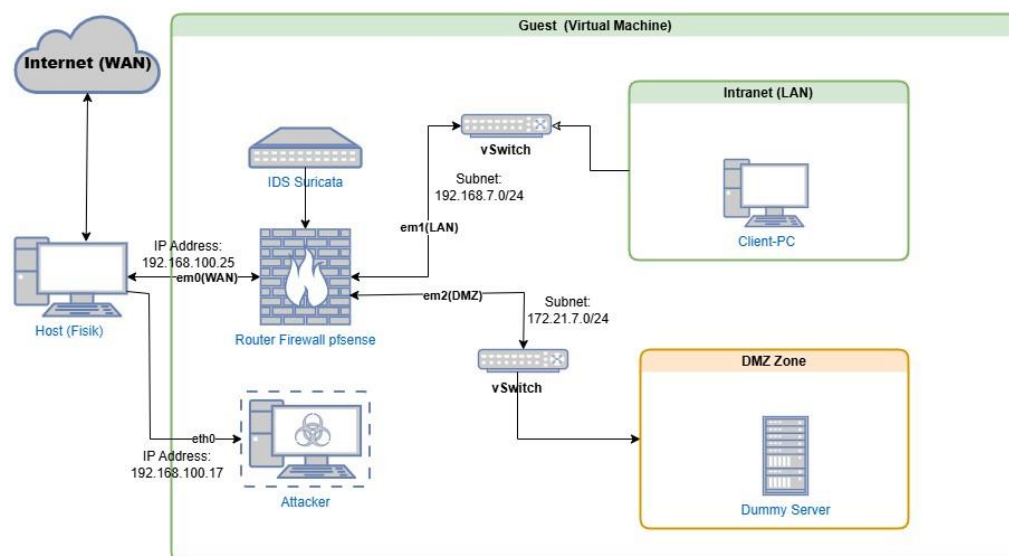


Fig. 1: Network security system architecture topology

Figure 1 visualizes the topology design results of a multihome network system simulation model with three network segments, namely WAN, LAN, and DMZ. This model is implemented in a virtual environment using the VMware Workstation hypervisor application. The system is built using several virtual machines, each with different functions, namely as a firewall (pfSense), dummy server (CentOS), and client (Windows). Hardware and software specifications have been adjusted to support the simulation, such as the use of a physical laptop with 16 GB RAM and 256 GB SSD, as well as resource allocation for each VM based on the role and workload of the simulation.

## 2.2. System Implementation

In the system implementation, the process carried out at this stage is to configure the devices in the network security system, including the main device of the pfSense firewall.

### a. Network interface configuration

Configuring the three main interfaces on pfSense, namely WAN, LAN, and DMZ. The WAN interface serves as the main link to the external network and acts as NAT for the DMZ server. The LAN interface is used to manage internal network traffic, while DMZ is intended to isolate servers that can be accessed by the public from the internal network. In addition, it configures other devices such as servers, client PCs, and attacker devices.

**Table 1:** Description of devices on the network

Device	Interface	IP Address	Description
VM Pfsense	em0 (WAN)	192.168.100.25/24	Connection to the internet and NAT of the DMZ server's public IP.
	em1 (LAN)	192.168.7.1/24	Handle internal network.
	em2 (DMZ)	172.21.7.1/24	Isolate the server from the internal network.
VM PC Client	ethernet	192.168.7.10/24	End-user in the internal network.
VM Server	ens32	172.21.7.10/24	Dummy server as a service provider.
VM Attacker	eth0	192.168.100.17/24	Acts as an attacker against the network system.

The data in Table 1 shows a description of the allocation and function of each resource in the network security system. The IP configuration applied is static for LAN and DMZ, while WAN is configured using DHCP. This setting aims to ensure secure and well-managed network segmentation. Then on the PC client, server, and attacker devices using DHCP mode.

### b. Firewall rules configuration

NAT port forwarding is applied to redirect traffic from the public IP address to the private IP address of the server in the DMZ. This configuration uses the port redirection method for services available on the server, thus strengthening the protection of the internal network. These rules can include only allowing certain types of traffic, as well as restricting access to certain ports. By carefully managing these firewall rules, organizations can improve their overall security posture while still allowing necessary communication with external users. Some descriptions of the rules that have been created can be seen in table 2 below.

**Table 2:** Firewall rule configuration

Rules	Terms	Description
NAT port forwarding	Has one rule that will handle requests from external networks.	With the rule that any access to the WAN IP address (192.168.100.25) will be directed or redirected to the server IP address in the DMZ segment.
Interface WAN	The interface has two rules. The first rule will handle inbound and outbound traffic requests to the DMZ server (NAT port forwarding rule). The second rule acts as a gateway that will handle internet connections for all networks (LAN and DMZ).	On the WAN interface, NAT port forwarding rules are applied to allow access to the DMZ server as well as outbound rules for internet access.
Interface LAN	The interface has two rules. The first rule will handle internet connections for LAN networks with specific ports. The second rule will act to handle ICMP packet requests for the LAN network.	Rules are created, including permission to access the internet for devices on the internal network (LAN). Destination ports are restricted, allowing only HTTP, HTTPS, and DNS ports. The firewall allows ICMP packets for ping purposes on the network.
Interface DMZ	The interface has two rules. The first will act to isolate the server in the DMZ from the internal LAN network. The second rule will host the internet connection for resources on the DMZ network.	At the DMZ interface, firewall rules are designed to prevent access to the LAN but still allow connection to the internet and allow the LAN to access services on the DMZ server.

### c. Implementation of IDS rule signatures

IDS implementation is done by installing the Suricata package on pfSense. Suricata is configured to inspect all traffic on WAN, LAN, and DMZ interfaces with the Emerging Threats Open (ET Open) ruleset. The signature ruleset will be used or applied to the Suricata IDS system. The ruleset contains a signature of common attack patterns that have been recognized before.

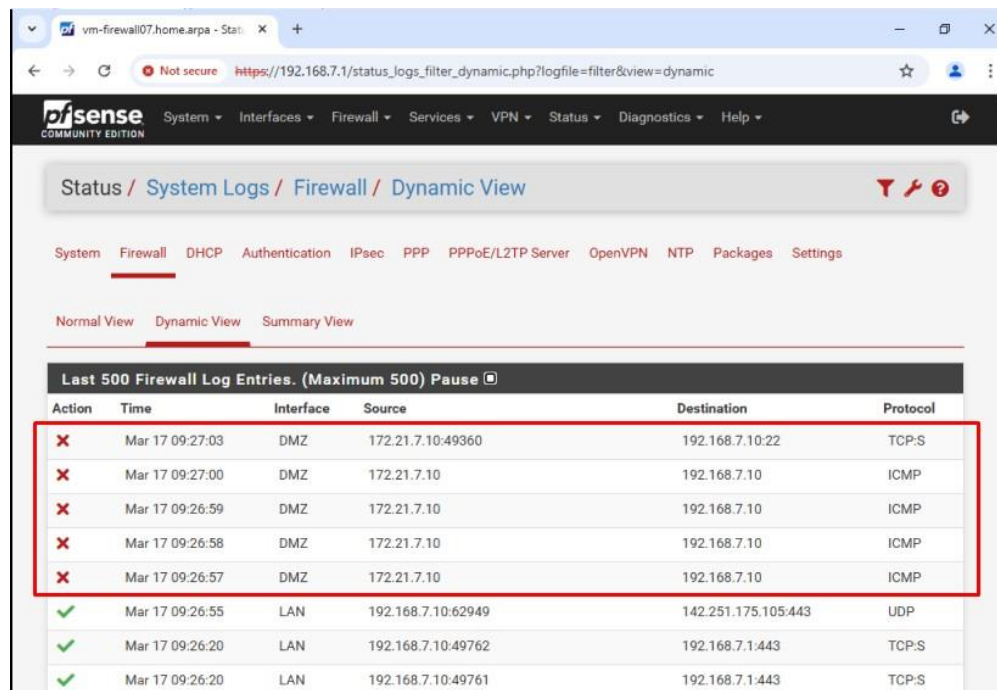
## 2.3. System testing

In the system testing phase, access testing and several types of attack patterns that commonly occur in a system, including network systems. Some types of attacks used in system testing, such as Denial of Service (DoS) using hping3, port scanning using nmap, and brute force attacks using hydra through attacker devices with Kali Linux operating systems. The attack is shown to the public IP of the DMZ server (192.168.100.25). This attack aims to test the system that has been implemented previously.

In addition to testing the attack, the process of testing access to one of the devices on the internal network is carried out to test whether the firewall rules that have been applied previously work according to the procedure. The rule being tested is blocking access of resources in the DMZ to the internal network (LAN) to ensure that servers in the DMZ are isolated from the internal network.

## 2.4. Log Collection

The log collection process carried out in this research is by monitoring the logging carried out by the firewall and also the IDS system that has been previously implemented. This is done to monitor system performance in handling an attack or suspicious activity on the network system. The log in question is a collection of digital footprint records recorded by the system so that it becomes material in analyzing whether an attack or unauthorized access to the system has occurred.



Action	Time	Interface	Source	Destination	Protocol
✗	Mar 17 09:27:03	DMZ	172.21.7.10:49360	192.168.7.10:22	TCP-S
✗	Mar 17 09:27:00	DMZ	172.21.7.10	192.168.7.10	ICMP
✗	Mar 17 09:26:59	DMZ	172.21.7.10	192.168.7.10	ICMP
✗	Mar 17 09:26:58	DMZ	172.21.7.10	192.168.7.10	ICMP
✗	Mar 17 09:26:57	DMZ	172.21.7.10	192.168.7.10	ICMP
✓	Mar 17 09:26:55	LAN	192.168.7.10:62949	142.251.175.105:443	UDP
✓	Mar 17 09:26:20	LAN	192.168.7.10:49762	192.168.7.1:443	TCP-S
✓	Mar 17 09:26:20	LAN	192.168.7.10:49761	192.168.7.1:443	TCP-S

Fig. 2: PfSense firewall logs

Figure 2 shows the results of logs carried out by the pfSense firewall system, where logs marked with red boxes indicate unauthorized access activity on the system. The log shows an attempt to request ICMP (ping) and SSH (port 22) with the destination host on the internal network (LAN). The firewall system immediately blocked the request because it violated the rules applied earlier to ensure that resources in the DMZ remain isolated from the LAN internal network.

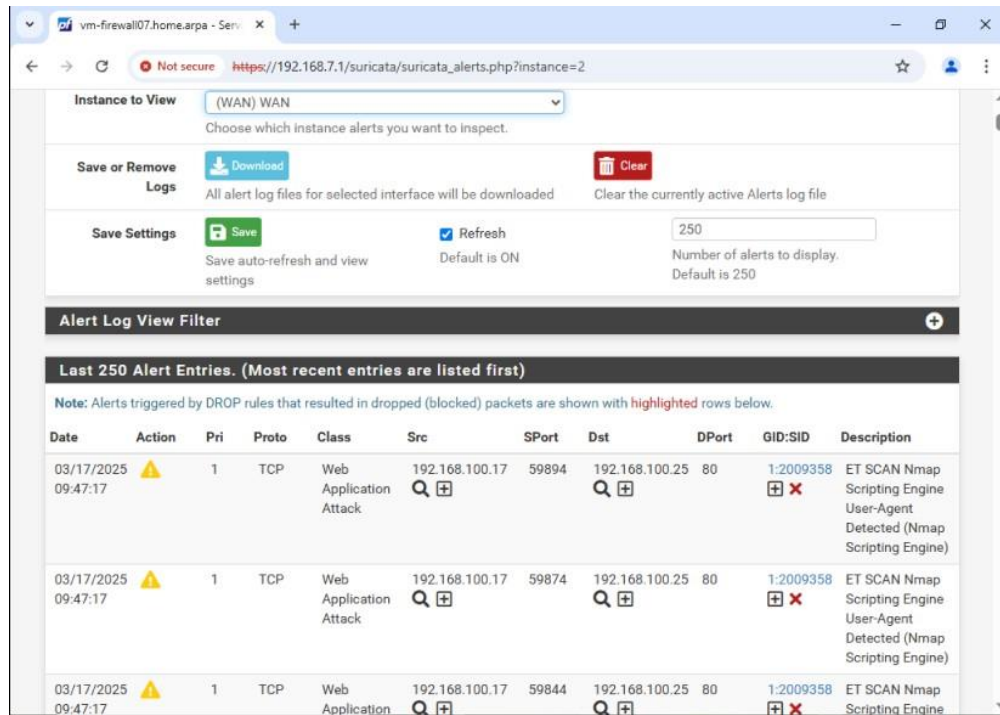


Fig. 3: IDS suricata system logs

Figure 3 shows the logs generated by the Suricata intrusion detection system. The system detects attacks with signature patterns that are in the installed ruleset (ET Open). The system is responsive in detecting attacks whose signature patterns match the system's ruleset, thus providing alerts to attacks in real time.

### 3. Result and Discussion

#### 3.1. Firewall System Analysis

The implementation of the pfSense-based multihome firewall shows effectiveness in managing network segmentation and access settings based on interfaces. The success of NAT port forwarding shows that the system is able to direct external requests to the DMZ server without exposing the internal network. Isolation between DMZ and LAN is also effective according to the firewall configuration implemented. This study successfully achieved its objectives based on the log results collected earlier, where this study was able to implement a multihome firewall with pfSense, implement network segmentation using the DMZ concept, and integrate Suricata-based IDS to improve network security in detecting various attacks. Multihome firewall system analysis is carried out to monitor system performance, both in handling abnormal activities on the network and normal activities in accordance with predefined rules.

Table 3: Pfsense firewall functionality testing

Testing Parameters	Testing Results
Authorized user access	Successfully, the user can access the authorized services.
Unauthorized user access	Blocked, unauthorized access attempts prevented by pfSense firewall.
Network segmentation (WAN, LAN, DMZ)	Functioning, each segment is under control according to the firewall rules.
System logging	All activity is properly recorded and stored in the pfSense firewall logs.

Table 3 presents the results of testing the pfSense firewall system in handling network traffic. The firewall system is able to filter data traffic on the network strictly, and maintaining system integrity is guaranteed. The pfSense-based multihome firewall shows solid performance in filtering network traffic based on preconfigured security rules. The system is able to recognize and block any unauthorized access attempts consistently, while legitimate traffic can still pass through the firewall unhindered. This shows that the filtering mechanism works in accordance with the expected network protection function.

#### 3.2. IDS System Analysis

The results of implementing IDS Suricata integrated with the pfSense firewall can improve network security. Suricata IDS will inspect traffic passing through each interface (WAN, LAN, and DMZ) according to the signature ruleset applied or enabled in the implemented network security system. IDS will filter incoming traffic through the pfSense firewall and match the data traffic pattern signature with the active ruleset. If a match is found, the IDS system will trigger an alert for abnormal traffic patterns.

Table 4: IDS system testing

Attack	Trial to	Attack Time	Alert Status	IDS Response Time
DoS Attack	1	09:29:05	Detected (true positive)	09:29:05
	2	09:33:45	Detected (true positive)	09:33:45
	3	09:36:10	Detected (true positive)	09:36:10
	4	09:39:50	Detected (true positive)	09:39:50
	5	09:42:10	Detected (true positive)	09:42:10

Attack	Trial to	Attack Time	Alert Status	IDS Response Time
Nmap Scan	1	09:47:17	Detected (true positive)	09:47:17
	2	09:49:30	Detected (true positive)	09:49:20
	3	09:52:40	Detected (true positive)	09:52:40
	4	09:55:25	Detected (true positive)	09:55:28
	5	09:58:00	Detected (true positive)	09:58:01
Brute Force Attack	1	10:10:15	Detected (true positive)	10:10:16
	2	10:14:05	Detected (true positive)	10:14:06
	3	10:18:50	Detected (true positive)	10:18:50
	4	10:21:40	Detected (true positive)	10:21:40
	5	10:25:20	Detected (true positive)	10:25:20

Table 4 shows the results of testing the IDS system with various types of attacks that commonly occur. In the test, the alert results generated by the IDS system are true positives (detected by providing an alert). The IDS system detects attack patterns in real time. These results are obtained by sorting out several relevant rulesets to mitigate the IDS system. Suricata produces false positives (provides alerts, but no attacks occur). The IDS system provides significant performance in detecting various types of attacks, it can be seen from several times of attack trials that the IDS system successfully detects without the discovery of false negatives.

## 4. Conclusion

Based on the research results, network security can be significantly improved by combining IDS Suricata, DMZ, and pfSense-based multihomed firewall. Network segmentation based on strict firewall rules is successfully implemented by the system, using DMZ to isolate publicly accessible services from internal resources from being exposed and using signature-based IDS rulesets to detect various common network attacks in real-time. The results of several experiments showed consistency against unauthorized access attempts in generating accurate alerts by the IDS without any false negatives. The implemented system is effective in mitigating by detecting common threats such as DoS, port scanning, and brute force attacks. However, there are still some false positives, and the system does not include Intrusion Prevention System (IPS) capabilities, which can strengthen real-time protection. Future work should focus on integrating IPS functionality and conducting evaluations against actual network environments.

## References

- [1] X. Z. Wei Jia, Cuiping Shi, "Automatic Translation of English Terms for Computer Network Security Based on Deep Learning," *J. Electr. Syst.*, vol. 20, no. 3s, pp. 598–609, 2024, doi: 10.52783/jes.1335.
- [2] J. Zhang, H. Feng, B. Liu, and D. Zhao, "Survey of Technology in Network Security Situation Awareness," *Sensors*, vol. 23, no. 5, pp. 1–25, 2023, doi: 10.3390/s23052608.
- [3] I. Cloudflare, "DDoS Threat Report for Q4 2024," Cloudflare Radar. Accessed: Feb. 05, 2025. [Online]. Available: <https://radar.cloudflare.com/reports/ddos-2024-q4>
- [4] Z. Wang, C. Zhang, Y. Ding, H., "Applied Mathematics and Nonlinear Sciences," *Appl. Math. Nonlinear Sci.*, vol. 8, no. 2, pp. 3383–3392, 2023.
- [5] P. Peng, "Research on Computer Network Security Vulnerabilities and Encryption Technology in Cloud Computing Environment," *Appl. Math. Nonlinear Sci.*, vol. 9, no. 1, pp. 1–17, 2024, doi: 10.2478/amns-2024-0171.
- [6] F. Zhao, "Computer System Security and Power Data Network Integrated Security Strategy Analysis and Optimization," *J. Netw. Comput. Appl.*, vol. 10, pp. 14–19, 2025, doi: 10.23977/jnca.2025.100103.
- [7] M. Zajeganović, "pfSense Router and Firewall Software," *Sint. 2023-International ...*, 2023, [Online]. Available: <https://portal.sinteza.singidunum.ac.rs/paper/918>
- [8] J. Huang, D. Zhang, S. Yang, M. Jia, H. Jiang, and X. Du, "Safety Monitoring Scheme of Gas Pipeline Network Based on Multi-homing Technology," *Adv. Eng. Technol. Res.*, vol. 9, no. 1, p. 119, 2023, doi: 10.56028/aetr.9.1.119.2024.
- [9] H. W. Oleiwi, N. Saeed, H. L. Al-Taie, and D. N. Mhawi, "Evaluation of Differentiated Services Policies in Multihomed Networks Based on an Interface-Selection Mechanism," *Sustain.*, vol. 14, no. 20, 2022, doi: 10.3390/su142013235.
- [10] S. Praptodiyono, T. Firmansyah, M. H. Anwar, C. A. Wicaksana, A. S. Pramudyo, and A. Al-Allawee, "Development of Hybrid Intrusion Detection System Based on Suricata With Pfsense Method for High Reduction of Ddos Attacks on Ipv6 Networks," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 9(125), pp. 75–84, 2023, doi: 10.15587/1729-4061.2023.285275.
- [11] W. Buqing, "Analysis of a new firewall constructed on Pfsense with Snort to defend against common internet intrusions," *Appl. Comput. Eng.*, vol. 43, no. 1, pp. 244–250, 2024, doi: 10.54254/2755-2721/43/20230841.
- [12] H. Abdulameer, I. Musa, and N. S. Al-Sultani, "Three level intrusion detection system based on conditional generative adversarial network," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 2240–2258, 2023, doi: 10.11591/ijece.v13i2.pp2240-2258.
- [13] Dhuha Sabri Ghazi, H. S. Hamid, M. J. Zaiter, and A. S. Ghazi Behadili, "Snort Versus Suricata in Intrusion Detection," *Iraqi J. Inf. Commun. Technol.*, vol. 7, no. 2, pp. 73–88, 2024, doi: 10.31987/ijict.7.2.290.
- [14] A. D. Saleem and A. A. Abdulrahman, "Attacks Detection in Internet of Things Using Machine Learning Techniques: a Review," *J. Appl. Eng. Technol. Sci.*, vol. 6, no. 1, pp. 684–703, 2024, doi: 10.37385/jaets.v6i1.4878.
- [15] D. Rahmat, I. Suherman, Z. Muharraran, and A. Khotimah Husna, "Perancangan De-Militarized Zone (Dmz) Area Berbasis Intrusion Detection System (Ids) Pada Infrastruktur Jaringan Komputer," *INFOTECH J.*, vol. 10, no. 1, pp. 1–11, 2024, [Online]. Available: <http://ecgalery.blogspot.co.id/2011/01/dmz->
- [16] S. Somantri, R. Zulkarnaen, and Gina Purnama Insany, "Design and Build a Network Security System Using Port Knocking, DMZ and IDS Techniques at SMA Negeri 1 Warungkiara," *J. Informatics Telecommun. Eng.*, vol. 7, no. 1, pp. 292–307, 2023, doi: 10.31289/jite.v7i1.9674.
- [17] N. I. C. Mat, N. Jamil, Y. Yusoff, and M. L. M. Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," *J. Cybersecurity*, vol. 10, no. 1, pp. 1–18, 2024, doi: 10.1093/cybsec/tyad023.
- [18] H. Najafi Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset," *Appl. Sci.*, vol. 14, no. 3, 2024, doi: 10.3390/app14031044.
- [19] D. Silva, J. Rafael, and A. Fonte, "Virtualization Maturity in Creating System VM: An Updated Performance Evaluation," *Int. J. Electr. Comput. Eng. Res.*, vol. 3, no. 2, pp. 7–17, 2023, doi: 10.53375/ijece.2023.341.
- [20] T. Dmytro, Y. Vasyly, T. Vitaliy, and N. YATSKIV, "INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION," *Int. Sci. J.*, no. 4, pp. 215–220, 2024, doi: 10.31891/2219-9365-2024-80-26.