PERFORMANCE EVALUATION OF PFSENSE IN DETECTING AND PREVENTING NETWORK ATTACKS IN CONTROLLED ENVIRONMENTS

Nemanja Jeličić*,
[0009-0004-2302-204X]

Marko Šarac
[0000-0001-8241-2778]

Singidunum University,
Belgrade, Serbia

Abstract:

In the contemporary digital landscape, network security represents a critical challenge due to the increasing frequency and sophistication of cyberattacks. Firewall systems play a central role in protecting network infrastructure by filtering traffic and controlling access. pfSense, an open-source firewall solution based on the FreeBSD platform, offers a wide range of features, including VPN, IDS/IPS, and advanced traffic control mechanisms.

This paper analyzes the effectiveness of the pfSense system in detecting and preventing various types of network attacks through experimental testing in both virtual and physical environments. The experiments encompass port scanning, brute-force attacks, and DDoS scenarios, utilizing tools such as Nmap, Hydra, and hping3. Research results indicate that pfSense, with properly configured IDS/IPS systems, can effectively detect and block a significant percentage of attacks, making it a reliable solution for network protection, particularly in resource-constrained environments.

Keywords:

Pfsense, Firewall, IDS/IPS, Network Security, Experimental Analysis.

INTRODUCTION

In today's digital environment, where information and communication technologies play a vital role across all spheres of society, information security has become highly relevant. Attempts to attack information systems are becoming more frequent and diverse, requiring advanced protective measures to preserve data integrity, confidentiality, and availability [1].

As a fundamental component of network protection, the firewall plays an essential role in traffic filtering, access control, and threat detection. In this context, pfSense stands out as one of the most popular open-source solutions, combining flexibility, scalability, and high functionality.

pfSense is a platform based on the FreeBSD operating system that enables the implementation of various security mechanisms, including firewall rules, VPN services, and IDS/IPS systems [2].

Correspondence:
Nemanja Jeličić

e-mail:
njelicic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2026-354-359

This paper analyses the efficiency of the pfSense system in protecting computer networks through experimental evaluation in controlled environments. The goal is to determine the extent to which pfSense can detect and prevent various network attacks and to assess its applicability in real-world environments with limited resources.

2. METHODOLOGY

2.1. RESEARCH METHODS

The data for this research were collected through the analysis of technical documentation and by conducting experiments in a controlled network environment. The experiments were carried out in two phases: in a virtual environment using Oracle VirtualBox and in a physical network environment.

The following methods were applied:

- Analytical method - for understanding the functionality of the pfSense system
- Comparative method - for comparing pfSense with other solutions
- Experimental method - for testing the system under real attack scenarios

2.2. ATTACK TYPES

To analyse the security mechanisms, standard network security testing scenarios were used:

- Port scanning attacks, performed using tools such as Nmap, represent a fundamental step in identifying network infrastructure [3].
- Brute-force attacks, typically executed using tools such as Hydra, are used to attempt unauthorized access to systems [4].
- DDoS attacks, including SYN flood and HTTP flood scenarios, represent one of the most common threats to system availability [4].

These attack scenarios were selected because they reflect common real-world threats and enable detailed analysis of firewall system responses across varying load and configuration conditions.

3. EXPERIMENTAL ENVIRONMENT

The experimental environment is crucial to this research, as it enables practical evaluation of the pfSense system under both controlled and realistic conditions. To obtain relevant results, experiments were conducted in two environments: virtual and physical.

This approach allows for a detailed analysis of system behaviour under isolated conditions and validation in real-world network environments.

To ensure a realistic experimental setup, the network architecture was designed to simulate a typical segmented environment consisting of WAN, LAN, and DMZ zones. The pfSense system acted as a central firewall and routing device connecting all network segments.

The virtual environment included four machines with clearly defined roles. The pfSense system was configured with three network interfaces: WAN for external connectivity, LAN for internal communication, and DMZ for hosting publicly accessible services. This segmentation enabled controlled testing of network security mechanisms and isolation of potential threats.

The Ubuntu Server was deployed in the DMZ zone and configured with Apache and SSH services, representing a typical target system exposed to external access. Kali Linux was used as the attacking machine, generating network traffic and executing different types of attacks. Windows 10 was used as a client system for administration and monitoring purposes.

This architecture allowed precise control over traffic flow and enabled detailed observation of system behaviour during attack scenarios, ensuring reliable and reproducible experimental results.

3.1. VIRTUAL ENVIRONMENT

The experimental setup is based on a virtual infrastructure that provides full isolation and control over test scenarios.

Table 1. Experimental Environment Configuration

Component	Virtual Environment	Physical Environment
Firewall	pfSense 2.8.0	pfSense 2.8.0
IDS/IPS	Snort	Suricata
Attacker	Kali Linux	Kali Linux
Server	Ubuntu Server (Apache, SSH)	Ubuntu Server (Apache, SSH)
Client	Windows 10	Windows 10
Network	VirtualBox Internal Network	Physical LAN/DMZ network

Virtualization enables the safe execution of various attack types without risk to real systems, which is particularly important in educational and research environments.

The network architecture consists of four virtual machines: pfSense, Kali Linux, Ubuntu Server, and Windows 10.

pfSense (version 2.8.0) acts as the central security device with three network interfaces:

- WAN - connected to the Internet via NAT
- LAN - internal client network
- DMZ - network segment for server services

Ubuntu Server is located in the DMZ and serves as the target system, running Apache and SSH. Kali Linux is used as the attacking system, while Windows 10 is used for administration via the pfSense web interface.

Communication between network segments occurs through pfSense, which filters traffic based on defined firewall rules. This segmentation allows for clear separation of network zones and the simulation of real security scenarios.

3.2. PHYSICAL ENVIRONMENT

After conducting experiments in the virtual environment, testing was extended to a physical network environment to validate results under more realistic conditions.

The physical network topology closely mirrors the virtual setup, with pfSense serving as the central firewall with three network interfaces: WAN, LAN, and DMZ.

In this environment:

- Windows 10 is used as the client
- Kali Linux as the attacker
- Ubuntu Server as the target system

Unlike the virtual environment where Snort was used, the physical environment uses Suricata, which provides improved performance and multi-threaded traffic analysis.

The experimental scenarios remained the same as in the virtual environment, which allows for direct comparison of results and analysis of system behaviour under different operating conditions.

3.3. IDS/IPS CONFIGURATION

The IDS/IPS configuration was implemented in both experimental environments using different tools.

In the virtual environment, Snort was used as the intrusion detection and prevention system. Snort operates based on predefined rules that enable the identification of known attack patterns and suspicious network traffic [5].

Snort was configured in Legacy Blocking mode, ensuring stable operation and reducing false positives.

In the physical environment, Suricata was used, offering improved performance through multi-threading and deeper packet inspection. It enables more efficient processing of large volumes of traffic and better detection of complex attacks [6].

The rules used in both systems include sets for detecting network scanning, brute-force attacks, and web attacks, thereby ensuring broad coverage of different types of threats.

In order to better understand the role of these systems, it is important to distinguish between IDS and IPS functionalities. While IDS operates in a passive mode by monitoring traffic and generating alerts, IPS actively blocks malicious traffic in real time. This distinction directly affects the overall effectiveness of the system, especially in environments exposed to frequent attacks.

In addition to signature-based detection, modern IDS/IPS systems may also implement anomaly-based techniques, which allow the identification of previously unknown threats. However, such approaches often require more complex configuration and may generate a higher number of false positives.

A comparison between the two implemented solutions further highlights their differences. Snort is widely adopted due to its simplicity and extensive community support. It is particularly suitable for smaller environments and virtualized systems where traffic volume is limited. However, its single-threaded architecture may reduce efficiency when processing large amounts of network traffic.

Suricata, on the other hand, introduces multi-threading capabilities, enabling better utilization of modern multi-core processors. This allows improved performance in high-throughput environments and makes it more suitable for deployment in real-world network infrastructures.

4. RESULTS AND ANALYSIS

Experimental testing of the pfSense system was conducted using multiple attack scenarios to assess its ability to detect and prevent various network threats. The results were collected through IDS/IPS system logs, as well as through the analysis of network traffic behaviour during the attacks.

The results were analysed separately for the virtual and physical environments to enable an objective assessment of the system's performance under different operating conditions.

4.1. PORT SCANNING ATTACKS

During a port-scanning attack in a virtual environment using the Nmap tool, the system successfully detected the scanning attempts through Snort rules, generating alerts and blocking suspicious IP addresses. The results show that pfSense can effectively identify network mapping attempts, which is the first step in most attacks.

Additionally, log analysis revealed that the IDS system recognizes different types of scans, including TCP SYN scans and stealth scans, enabling more precise detection of potential attackers.

The detection efficiency in this scenario was high, and the system's response was timely, confirming the importance of properly configured rules in the IDS/IPS system. In the physical environment, detection was similar, but the system operated more stably with fewer false positives.

4.2. BRUTE-FORCE ATTACKS

Brute-force attacks conducted with the Hydra tool demonstrated that the IDS/IPS system can detect numerous unauthorized access attempts.

However, the effectiveness of blocking depends on the system configuration and the IDS/IPS operating mode. In certain cases, detection was successful, but blocking was not immediate, indicating a need for rule optimization, which is in line with known challenges of IDS systems, such as false positive detections [7].

During testing, the system generated numerous alert messages indicating repeated authentication attempts, enabling the administrator to identify an attack early. Additionally, the difference between IDS and IPS modes significantly affects the final outcome of an attack, as IDS only detects attacks, whereas IPS enables active traffic blocking.

During testing in a virtual environment, attack detection was reliable, but blocking was not always immediate. In a physical environment using the Suricata system, more efficient processing of a higher number of requests in real time was observed.

4.3. DDOS ATTACKS

In the event of a DDoS attack, including SYN flood and HTTP flood scenarios, pfSense demonstrated the ability to detect abnormal traffic. The system successfully identified an increased number of requests and generated appropriate logs, but the effectiveness of protection depended on available hardware resources and firewall rule settings.

During a SYN flood attack, a significant increase in half-open connections was observed, which is a typical indicator of this type of attack.

In the HTTP flood scenario, the system recorded increased load on the web server, with detection being successful, but complete mitigation required additional adjustments and rule optimization.

These results indicate that pfSense can detect DDoS attacks, but its efficiency in prevention depends on system configuration and available resources.

In a virtual environment, limitations were noticeable due to virtual machine resources, whereas in a physical environment, the system exhibited more stable behaviour and better network traffic handling.

4.4. RESULTS

The results indicate that pfSense can successfully detect most of the analysed attacks, while the level of prevention depends on the proper configuration of IDS/IPS mechanisms and system resources.

It has been observed that the system achieves the best efficiency in detecting port-scanning attacks, while brute-force and DDoS scenarios show greater dependence on configuration and hardware capacity.

In general, the results in the physical environment showed greater stability and reliability compared to the virtual environment, which is expected due to differences in resources and the way the system operates.

The results shown in Table 2 allow for a direct comparison of the system's efficiency in the virtual and physical environments.

Table 2. Comparative overview of attack detection and prevention

Attack Type	Virtual environment detection	Virtual environment prevention	Physical environment detection	Physical environment prevention
Port scanning	High	High	High	High
Brute-force	High	Medium	High	High
DDoS	Medium	Limited	High	Medium

The obtained results highlight the importance of proper system configuration and rule tuning. While detection capabilities are generally high across all tested scenarios, prevention effectiveness varies depending on the complexity of the attack and the available system resources.

The experiments also demonstrate that combining multiple security mechanisms, such as firewall rules and IDS/IPS systems, significantly improves the overall level of network protection. This layered approach is considered a best practice in modern cybersecurity architectures.

This confirms that a layered security approach significantly enhances the resilience of network infrastructure against a wide range of attack vectors. Such an approach is particularly important in modern network environments where threats are increasingly complex and dynamic.

5. SYSTEM PERFORMANCE EVALUATION

The obtained results indicate that the pfSense system can effectively detect a wide range of network attacks under controlled conditions. It particularly stands out for its high efficiency in detecting port-scanning activities, as the system quickly identifies suspicious traffic patterns.

For more complex attacks, such as brute-force attempts, it has been observed that effectiveness depends on the configuration of IDS/IPS rules and the system's operating mode. In this context, proper rule configuration and the selection of an appropriate operating mode are crucial to achieving optimal protection.

In scenarios of increased load, such as DDoS attacks, system performance directly depends on available hardware resources, which confirms that pfSense, as a software-based solution, requires adequate hardware support, in line with modern research in network attack detection [8].

The advantage of the system lies in its flexibility and ability to adapt to different network scenarios, while the limitations stem from the need for advanced configuration and administrator experience.

Another important aspect is scalability. In larger network environments, the ability of the system to maintain consistent performance becomes critical. This further emphasizes the need for adequate hardware resources and optimized configuration settings.

Despite these limitations, pfSense remains a highly adaptable solution that can be deployed in a wide range of scenarios, from small enterprise networks to more complex infrastructures.

6. CONCLUSION

The results confirm that pfSense represents an efficient and flexible solution for protecting computer networks in controlled environments [2].

The integration of IDS/IPS systems enables the detection and prevention of various types of attacks, including port scanning, brute-force, and DDoS attacks.

Although system performance depends on hardware resources and configuration, pfSense proves to be a reliable alternative to commercial firewall solutions, particularly in environments with limited budgets.

Future research may focus on IDS/IPS rule optimization and improving system performance under high network load conditions.

REFERENCES

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," *Computer Communication Review*, vol. 19, no. 2, p. 32–48, 1989.

[2] Netgate, "pfSense Documentation," 2024. [Online]. Available: https://docs.netgate.com/pfsense/en/latest/.

[3] Nmap Project, "Nmap Reference Guide," 2023. [Online]. Available: https://nmap.org/book/man.html.

[4] OWASP Foundation, "Web Security Testing Guide," 2023. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/.

[5] Snort Project, "Snort User Manual," 2023. [Online]. Available: https://www.snort.org/documents.

[6] OISF, "Suricata Documentation," 2024. [Online]. Available: https://docs.suricata.io/en/suricata-8.0.4/.

[7] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *IEEE Symposium on Security and Privacy*, 2010.

[8] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Computer Communications,* pp. 1-17, 2014.