IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 April 2026, accepted 21 May 2026, date of publication 2 June 2026, date of current version 18 June 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3699458

RESEARCH ARTICLE

Performance Analysis of pfSense in Cyber Defense: An Intelligent Firewall Perspective for the Modern Network Landscape

V. ASHA AND S. KANAGA SUBA RAJA
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu 621105, India
Corresponding author: S. Kanaga Suba Raja (kanagass@srmist.edu.in)

ABSTRACT The primary goal of this research is to evaluate and compare the performance of pfSense as an open-source firewall and routing tool based on FreeBSD, with the enhancements made through machine learning to transform it into a proactive detector of emerging threats. This research utilized empirical testing of pfSense in both hardware and software based virtual environments. The results of this study showed measurable increases in some important network parameters, such as a 14.1% increase in network throughput (from 850 Mbps to 970 Mbps), a 52% decrease in packet loss (from 2.5% to 1.2%), and a 21.9% decrease in network latency (from 10.5 ms to 8.2 ms). While the results of this study identified improvements in both network and security related metrics.Specifically, the threat detection improved by 8% (from 89% to 97%), and the false-positive rates dropped by 44.7% (from 3.8% to 2.1%). In addition, the study evaluated the ability of the pfSense system to detect zero-day attacks and found that it improved by 17.3% (from 78.2% to 91.7%). The study also evaluated the impact of adding machine learning capabilities to the pfSense system and found that there was a significant decrease in the amount of computational resources required to operate the system; specifically, the CPU utilization dropped from 65% to 58%, and memory usage decreased from 72% to 64%. This study discusses how the SHAP and LIME techniques can be implemented into the pfSense architecture to improve transparency and accountability in the decision making process in security. In addition, this study provides a comparison between pfSense and traditional stateful inspection firewalls to demonstrate the differences in flexibility, operational costs, and adaptability to evolving threats. Overall, this study identified real-world, enterprise level problems associated with resource utilization and configuration complexities and demonstrated how pfSense provides a viable and scalable open-source security solution that can address the needs of organizations seeking flexible and adaptable network defense architectures.

INDEX TERMS pfSense, intelligent firewalls, cyber threat mitigation, network protection.

I. INTRODUCTION

The complexity of today's cyber world far exceeds the capabilities of conventional firewalls and their setups. Therefore, intelligent firewalls have become a key element in today's cybersecurity models. Intelligent firewalls provide the capability to inspect packets at multiple layers, filter traffic based on the layer of the application that the traffic is used with, support the creation of secure remote VPN connections, and support intrusion detection [1]. In this area, pfSense is one of the few examples of a highly configurable firewall and routing system [2].This article explores the various methods of installing and configuring pfSense and how well it serves as an intelligent firewall. Although pfSense provides numerous security related services, including packet filtering; however, it also allows organizations to develop custom security related services and implement them to satisfy their organizational and policy-based requirements [3]. For example, in the context of stateful packet inspection, pfSense only permits packets containing

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

valid data to pass through and rejects all packets lacking content. Additionally, the application-layer filtering function of pfSense provides organizations with the ability to exercise a finer degree of control over specific applications and services. Furthermore, the inclusion of AI-based add-on modules in pfSense provides organizations with additional means to analyze and protect themselves from potential security threats [4]. Therefore, the process of implementing pfSense as an intelligent firewall includes several deployment stages. First, it must be installed into either a dedicated hardware device or a virtual environment; secondly, the pfSense network interfaces must be configured; and thirdly, the pfSense firewall configuration must be developed to meet the security policies of the organization. One of the main factors that contribute to the ease of deploying and managing pfSense is its web-based Graphical User Interface (GUI), which is much simpler to manage and configure than most other firewalls [5]. PfSense may also be integrated with external threat feeds, high availability configurations, and load balancing configurations, to name a few, making it an attractive option for organizations having complex and large-scale networks.Therefore, this study evaluates the capabilities of pfSense by collecting empirical data to compare it with other types of firewalls. The findings demonstrate that pfSense offers organizations both flexibility and lower costs for addressing the increasing complexities of today's cybersecurity [6]. This study serves as an educational resource for organizations seeking to learn about emerging trends in intelligent firewalls and illustrates the need to utilize pfSense when developing robust, scalable, and flexible network architectures [7].

A. PFSENSE: INTELLIGENT FIREWALL

Figure 1 described in the paper outlines how the system utilizes an integrated system, including pfSense, AI, Data Driven Machine Learning (Data Driven ML), and an IDS to protect a trusted network from possible attacks, as referenced in [8]. Once the incoming data stream reaches the pfSense router, it extracts some of the data stream metadata and sends it to the Intelligent AI Module. The Intelligent AI Module uses the metadata and historical data to create a data stream traffic pattern, calculates a Risk Score for the data stream, and updates Security Policies based on the calculated Risk Score. Based on the risk score calculated by the Intelligent AI Module, it determines whether to permit the data stream to pass through to the trusted network, deny the data stream passage to the trusted network, or restrict the flow of the data stream to prevent unauthorized access to the trusted network. After the Intelligent AI Module has made the decision to allow the data stream to enter the trusted network, the IDS performs the final level of security analysis at the last point of defense before entry into the trusted network. To keep the Network Security Architecture current and to prevent delays, it needs to be updated periodically. The Network Security Architecture can be kept current and updated using the Operational Data generated while monitoring and maintaining it, which is then sent to the Data Driven ML Module to enhance the detection and response capabilities of the Network Security Architecture to new threats and improve its overall performance, as referenced in [9].

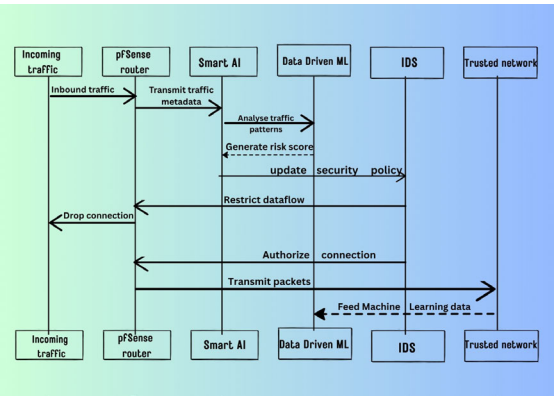

FIGURE 1. pfSense Firewall with AI and machine learning.

Figure 2 pfSense's extensive firewall features demonstrate why firewalls are such an essential element of current network security. Beginning with Net Ingress, as packets move across each interface, they are captured or recorded at that time while the Packet Sniffing Mechanisms examine the packet data itself. Following this analysis, a specific AI analyzes that data utilizing Machine Learning algorithms to evaluate Anomalies & Threat Assessments, thus identifying possible threats. After the data has been evaluated, the results are relayed to pfSense, the proprietary engine responsible for generating access rules throughout the firewall, including an IDS (Intrusion Detection System). The results of the system are utilized by the system results module to aid in decision making & response actions, tracking events, monitoring, and providing a graphical user interface (GUI) for the administrator to utilize in active security management & control of the security flow. A feedback loop exists when the results of the system are fed back into pfSense; the iterative policies are modified, and real-time threats are mitigated via operational feedback. This represents a combination of pfSense with artificial intelligence and machine learning; offering the operational flexibility and scalability of a powerful firewall to increase the network security of a client [10].

The remainder of this report is structured as follows: In Section II, I will review previous research that has studied the growth of network security to help understand what network security has been and what it has become over time. In Section III, I will define the importance and goals of the study. This includes (A) defining the scope of the study and its purpose, and (B) illustrating the benefits of using the proposed model to aid organizations. In Section IV, I will present the primary literature review and meta-analysis that will be used to find Algorithm 1: pfSense Network

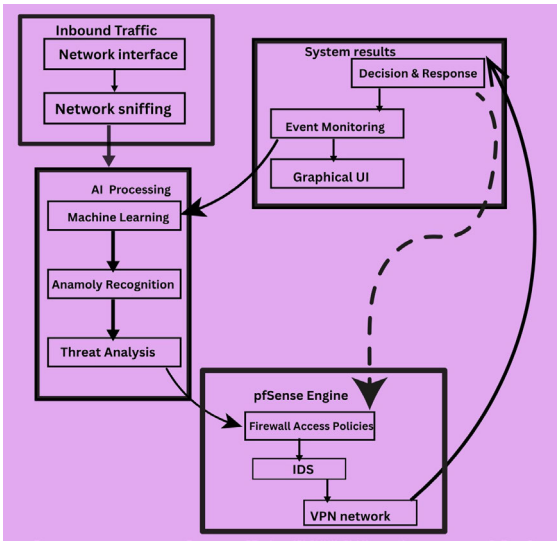

FIGURE 2. AI-Driven Network Security with pfSense Firewall.

Security. In Section V, I will define the methodology behind the study with respect to the use of pfSense as an intelligent firewall. In Section VI, I will describe how the system was implemented, specifically how the AI-enhanced pfSense firewall would detect advanced threats in real-time and enforce policies on network traffic continuously. In Section VII, I will analyze the experimental results and show how the proposed model improves both network performance and network security, as well as how AI optimization affects the performance of the pfSense firewall. Additionally, I will illustrate the trend of performance improvements in pfSense from baseline to AI-optimized configurations and compare the performance of pfSense to other firewalls in relation to performance metrics. In Section VIII, I will conclude the study and highlight why pfSense could be considered an important advanced open-source firewall for today's cyber-security issues, especially when AI is involved. In Section IX, I will propose future work related to pfSense, including developing new capabilities to counter future cyber-security issues and improving the performance of pfSense in dynamic networks. Finally, in Section X, I will outline the drawbacks of the proposed model, highlighting the limitations of pfSense as an advanced firewall, although it provides many benefits.

B. INTELLIGENT PFSENSE FIREWALL USING AI OPTIMIZATION

The proposed intelligent pfSense firewall framework is an AI-optimized network that can improve the security of a network by carefully designing a combination of diverse machine learning models, optimizing feature engineering, adaptive processing, and explainable AI units into a single framework. This optimization policy focuses on a trade-off that balances detection errors, inference latency, and computational resource utilization, which are vital parameters in current high-throughput network conditions. An architecture is a hierarchical cluster of models where lightweight algorithms such as Random Forest and XGBoost are strategically deployed to triage traffic in real-time based on packet-level and flow-level characteristics (like IP addresses, port numbers, protocol types, QoS markings, TCP flags, and connection states) to allow real-time classification with minimal latency. Convolutional Neural Networks and Long Short-Term Memory networks are more intensive models that are triggered on-demand to inspect and examine temporal behavior. The models are based on the encoded payload structure and distributions at the byte level, along with time-sequenced flow statistics (inter-arrival times, sequence numbers, and connection durations) to identify polymorphic, stealthy, and multi-stage attacks. This hierarchical implementation is an important AI optimization in which only suspicious traffic is sent to more complex models, thus avoiding needless deep processing. With only a minor loss in detection performance, overhead is greatly reduced. By using a multi-dimensional representation of packet-level, flow-level, and statistical features, the system maximizes feature utilization, making each model use the best subset of features, resulting in better generalization and reduced redundancy. The optimization is trained using large-scale benchmark data, grid search, and k-fold cross-validation to optimize hyperparameters, as well as real and synthetic attack scenarios, which makes it more robust and significantly improves zero-day attack detection abilities. It is built to be interoperable with pfSense using a highly-tuned multi-mode deployment approach, where lightweight models are run in real-time for inference and deep learning components are offloaded to external high-performance environments to deliver scalability and prevent resource bottlenecks in the firewall system [11]. It is an adaptive, parallelized traffic processing pipeline that works with packet capture, feature extraction, model inference, ensemble decision-making, and enforcement, and can be further optimized to use early-stage filtering and dynamic routing of inference to ensure very narrow latency limits. Besides optimizing performance, the framework also includes explainable AI techniques, such as SHAP and LIME, which are asynchronous and offer global and instance-level explainability without impacting real-time detection, thereby resolving the problem of AI-based security system transparency, which is highly crucial. These performance data indicate that this optimization approach not only improves the accuracy of detection but also saves CPU power, memory power, and energy, as well as reduces lost packets and improves throughput and overall network efficiency.

C. NETWORK TOPOLOGY AND SEGMENTATION

Figure 3 shows the Wide Area Network (WAN) section of this experimental multi-layered design of a real world enterprise environment that connects to simulated Internet services, which create both typical traffic patterns and representative external threats. The LAN segment includes several subnets

to host workstation clients, server resources, and network hardware devices. The DMZ section hosts publicly available services in the form of a web server, FTP server, and email server to identify potential attack points commonly found in most networks. All three segments are separated into different VLANs to isolate the traffic flow. VLAN 10 is utilized for traffic management, VLAN 20 for LAN operations, VLAN 30 for DMZ operations, and VLAN 40 for WAN connections. Because all communications that cross VLAN boundaries must pass through the pfSense Firewall Policy, all VLANs have unlimited routes for data transfer between them (except those defined by their respective policies). This allows full control over the flow of data and enforces strict security measures. Quality of Service (QoS) configurations were also implemented to prioritize critical applications and maintain reasonable application performance levels to simulate a realistic network performance evaluation.

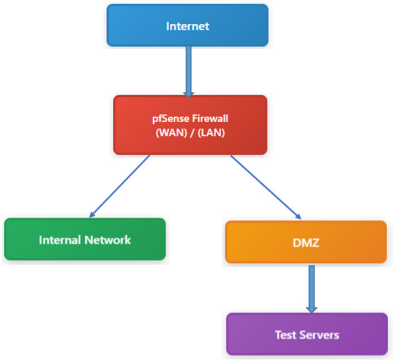

FIGURE 3. Network Topplogy:pfSense Firewall Landscape.

II. BACKGROUND

To offer network security that can protect against evolving threats, we must find ways to provide new protection mechanisms for networks. Because the sophistication of attacks is greater than what can be addressed by rule-based packet inspection, there is an increasing need for smart firewalls as organizational infrastructures transition from stand-alone systems to distributed network systems [12]. Modern firewalls use stateful packet inspection and application layer filtering. Intrusion Detection and Prevention Systems (IDPS) are even more sophisticated.

pfSense is one of the most popular firewalls and routing systems, primarily because pfSense is flexible and cost-effective.In addition, because pfSense is based on FreeBSD, it is supported by a larger community. Similar to other firewalls, pfSense has the core functionality needed to meet the needs of virtually any organization; however, unlike other firewalls, pfSense includes additional advanced features that can enhance both network speed and security. Some examples of the advanced features of pfSense include, but are not limited to, load balancing, traffic shaping, and captive portals [13].

The flexibility of pfSense as an architectural platform allows it to be implemented in almost any type of environment, from small organizations to large corporate environments, as well as in the creation of complex network systems, such as DMZ and HA configurations, because pfSense supports multiple WAN and LAN connections [14]. Numerous technological advancements have been made over the past decade that directly relate to how firewalls operate, partially due to the limitations of traditional ''rule-based'' security models that are simplistic. The newer and more complex types of threats include persistent zero-day attacks, polymorphic malware, and advanced firewalls that utilize weaponized vulnerabilities in static firewalls and non-adaptive flaws without behavior analysis. Consequently, the technology used to produce firewalls today includes intelligent threat systems and multi-layered security. Smart firewalls are quickly replacing traditional firewalls and providing more complex systems integration that enables dynamic decision making.

One of the key reasons that pfSense has become so prominent in this category of solutions is the multitude of features that pfSense offers, along with its modular design, which allows members of the security community to create and implement advanced firewall extensions. Although pfSense offers many benefits, it does not provide the capability in its standard configuration to address behavioral attacks, dynamically respond to changing conditions in real time, or pro-actively mitigate zero day exploits. Therefore, this study proposes to fill these gaps through the development of a smart, adaptive security framework that provides autonomous real-time security response capabilities and dynamically adjusts policies within the pfSense environment. An examination of the current literature indicates that although many prior studies have evaluated pfSense in terms of its performance in various deployment environments and have compared it with commercial firewall solutions, little attention has been paid to incorporating XAI techniques into the pfSense architecture. Specifically, there is no prior study that has assessed the concurrent improvement of both threat detection accuracy and decision transparency using SHAP and LIME techniques. This broad literature review sets the foundation for the proposed research framework and emphasizes the originality of the contributions to the area of intelligent firewall systems.

However, pfSense has several limitations that should be considered in operationally demanding networks. For instance, if a significant amount of traffic is being transferred over a network, additional hardware may need to be added to the system to allow pfSense to function at maximum efficiency and scale. pfSense uses an easy-to-use web-based GUI to configure and manage the system; however, those without a broad background in security may experience a learning curve when initially configuring pfSense. However, ongoing research and development are being conducted to improve pfSense's usability, scalability, and integration with artificial intelligence (AI) security technology that can

detect and respond to real-time threats [15]. Furthermore, the increase in APTs, Ransomware, and Zero Day Exploits has further emphasized the need for firewalls that can automatically enforce policies to counteract new threats. pfSense offers this capability by allowing users to create or modify rules and access external threat intelligence feeds to proactively mitigate threats. Therefore, as cyber threats continue to evolve and become increasingly complex, pfSense will remain an available and scalable open-source firewall solution for organizations seeking to improve their current network defenses [16].

III. RESEARCH CONTRIBUTIONS AND SIGNIFICANCE

The rise of increasingly complex cyber threats has exposed the shortcomings of existing stateful firewalls that rely on static, rule-based packet filtering. This study responds to the growing demand for intelligent and adaptable security solutions by evaluating an AI-enriched pfSense Firewall using an empirical approach. While pfSense is a widely known and cost-effective open source firewall, little scholarly attention has been given to the incorporation of machine learning and explainable artificial intelligence into pfSense. This study fills this void by conducting a systematic review of pfSense as an intelligent firewall to counter modern threats such as malware, phishing, Advanced Persistent Threats (APT), and Zero Day attacks within both the physical and virtual environments of an enterprise.

An important contribution of this study is the implementation of practical machine learning and explainable artificial intelligence methods, specifically SHAP and LIME, in an open-source firewall architecture. Although no new AI model is introduced in this study, it clearly shows that pfSense can be transformed into a self-adapting, dynamic, and interpretive security platform. The proposed framework increases threat detection accuracy, reduces the number of false positives, and makes the security decision-making process more transparent,enabling its use in enterprise environments where compliance and auditability requirements exist.In addition, this study presents statistical validation of performance and security metrics [17]. The controlled experiments demonstrated quantifiable improvements in network throughput, packet loss, latency, detection of zero-day exploits, and optimization of resource utilization. To validate the results, multiple independent trials were performed to create confidence intervals and to test for significance.

Another key contribution is filling the gaps in the literature concerning the use of AI-enhanced firewalls in enterprise environments. In addition to demonstrating the feasibility of using pfSense as an AI-enhanced firewall, the paper offers practical deployment guidelines related to hardware scalability, integrating legacy infrastructure, and operationally relevant considerations for the deployment of AI-enabled firewalls in an enterprise environment. An analysis of costs and business impacts shows that the total cost of ownership can be significantly lowered when using pfSense compared to meeting enterprise-grade security standards; therefore, this provides budget-constrained organizations with the opportunity to make informed decisions about the deployment of pfSense.

Finally, this study bridges the knowledge gap between commercial and open-source security platforms. By employing industry-standard penetration-testing tools, traffic generators, and multi-vector attack simulations, this paper removes the perception that open source firewalls are unsuitable for enterprise use. Moreover, the use of explainable AI in this research minimizes the ''black-box'' concern associated with AI-driven security systems and solidifies pfSense as a scalable, robust, and transparent solution for modern network defense.

This study explores pfSense as a high-performance platform and evaluates its capacity to enhance an organization's network security infrastructure [18]. This study assessed the primary functions of pfSense,including stateful packet inspection, intrusion detection/prevention systems, VPN capabilities, and application-layer filtering, to determine the extent to which they contribute to the strength of an organization's network protection. Performance testing was conducted on pfSense in both dedicated and virtualized hardware environments to assess its ability to prevent unauthorized access to an organization's network and mitigate various types of security threats. A comparative analysis of traditional stateful firewalls and other firewall solutions highlights the advantages of pfSense, including its flexibility, scalability, and cost effectiveness [19]. Additionally, this paper discusses the benefits of the open source framework and community-driven development model of pfSense. However, it also identifies the limitations of pfSense due to the need for hardware resources and the technical expertise required to configure some of pfSense's advanced features.

IV. LITERATURE ANALYSIS

The exponential growth in both the volume and sophistication of malicious cyber activity has resulted in a paradigm shift from rule-based to context-aware and adaptive firewalls that provide secure and adaptable security enforcement. Rule-based firewalls currently filter packets through fixed filters based on source and destination IP addresses, ports, and protocols [20]; however, they are limited in their capability to protect against today's sophisticated cyber threats. Stateful packet inspection, application-layer filtering, and IDS/IPS functions represent advanced technologies that enable intelligent firewalls to examine every layer of data and respond effectively to complex threats. pfSense, a free, open-source firewall and router software package developed on FreeBSD, is a popular option due to its modular structure, cost benefits, and numerous security-related features. It was originally created from the m0n0wall firewall project and uses the FreeBSD Packet Filter (PF) to perform stateful packet inspections [21]. It includes many other features, including IDS/IPS, VPNs, traffic shaping, load balancing, and captive portals. Therefore, pfSense is suitable for use in any organization [22].

As APTs, ransomware, and zero-day exploits are increasingly being used by adversaries to target organizations of all sizes, the demand for adaptive, self-configuring firewall products continues to increase. pfSense meets this challenge by enabling real-time dynamic firewall rule enforcement, supporting threat intelligence feeds, and real-time traffic validation. Studies investigating the performance of pfSense illustrate that it achieves excellent threat detection, VPN performance, bandwidth management, and failover, as illustrated in Table 1. Consequently, pfSense seems to be very robust across a wide array of network conditions.

Recently, researchers have emphasized the use of artificial intelligence (AI) to enhance the performance of pfSense. Specifically, AI-enabling components can enable real-time anomaly detection, adaptive policy enforcement, and proactive threat detection, especially concerning zero-day attacks and APTs. There are limitations, however, regarding the amount of hardware needed for deployment and the complexity of configuration; pfSense remains a powerful and flexible open-source security solution. Another open-source firewall gaining popularity as an alternative to pfSense is OPNsense. OPNsense focuses on ease-of-use, modern GUIs, and simplified deployments. Like pfSense, OPNsense integrates Suricata for IDS and supports multiple VPN protocols and traffic management capabilities. OPNsense has a plugin-based API and offers real-time visualizations to help administrators visually monitor their environment. Nonetheless, at present, OPNsense lacks the AI-based and explainable security models that are available in pfSense [23].Comparative studies examining open-source firewalls, including pfSense and OPNsense, versus commercial firewalls have demonstrated that when appropriately configured, they can match or surpass the detection capabilities of commercial firewalls and do so at less expense. Moreover, comparative studies have indicated that the utilization of explainable AI methodologies (such as SHAP and LIME) in intelligent firewalls may improve administrator confidence in AI-driven firewall decisions and mitigate uncertainty when administrators are deciding how to act based on AI-driven decision making. The literature is exhibiting an increasing trend toward the implementation of Zero-Trust Architectures (ZTAs) in firewalls, which advocate for continuous verification, micro-segmentation, and behavior-based policy enforcement. Machine learning enabled firewalls that are capable of continuing to learn about their environment and dynamically adjust their security posture based on the latest threat intelligence are examples of ZTAs compliant firewalls.

This study examined a broad spectrum of peer-reviewed publications and academic journals that investigated the evaluation of pfSense as a firewall product and intelligent techniques for enhancing the security of pfSense. We divided our review into five primary areas: (1) architectures and security platforms of open-source firewalls, (2) empirical methodologies for assessing the performance of network security devices, (3) applying artificial intelligence and machine learning to detect threats in real-time, (4) evaluation of IDS/IPS systems that employ Suricata and Snort, and (5) comparisons of open-source and proprietary firewalls in enterprise environments. The majority of the studies reviewed pfSense as a firewall product and investigated its performance, operational efficiency, and security enhancements. Both pfSense and other open-source firewalls address the growing needs for intelligent, adaptive defensive mechanisms to combat the complexities associated with cyber threats. Ongoing research aims to improve the detection accuracy, resource consumption, and cloud security integration of intelligent, adaptive firewalls. Open-source firewalls appear to hold a lot of potential for protecting networks in the next-generation by offering transparency, scalability, and improved security capabilities to a wide variety of industries. Advantages of open-source firewalls include cost savings, a high degree of customizability, real-time threat detection, and redundant fail-over capabilities; however, disadvantages include increased CPU/RAM requirements, increased complexity of configuration, and false positive rates in IDS [24].pfSense has become one of the most broadly utilized open-source firewall solutions, characterized by its modular structure, VPN support, traffic shaping, HA configuration, and seamless IDS/IPS system integration. pfSense's extensibility and flexibility make it an appealing alternative to proprietary firewalls. Research studies have validated the effectiveness of pfSense in both SMEs and large-scale enterprise settings. Unlike traditional static firewalls, pfSense employs the PF engine to facilitate efficient connection state management, traffic prioritization, and fault-tolerant multi-WAN configurations. Comparative studies have identified the cost-effectiveness and scalability of pfSense; nonetheless, pfSense requires additional hardware resources and presents a significant learning curve for users configuring complex setups. Researchers have recently focused on integrating AI/ML techniques into pfSense and OPNsense-based environments to enhance the detection accuracy and adaptive responses offered by pfSense. Studies have demonstrated the efficacy of AI/ML-integrated security models in improving anomaly detection, throughput, and zero-day attack detection, with detection accuracy gains of up to 17.3% being reported, validating the feasibility of AI-enhanced open-source firewalls in modern cybersecurity infrastructures.The recent studies on XAI techniques (e.g., SHAP and LIME) have been used to improve the interpretability and transparency of AI-driven security decisions. Previous research into using XAI techniques to enhance security decision-making through AI has primarily focused on experiments or simulations that did not provide standard, reproducible benchmarking for comparison. The primary objective of this current study is to empirically validate the security effectiveness, scalability, and cost-effectiveness of pfSense in modern network landscapes.

Table 1 compares the machine learning models implemented in the AI-optimized pfSense firewall, showing their

TABLE 1. Meta analysis.

Key Findings	Methods Used	Advantages	Disadvantages	Accuracy
pfSense demonstrated high throughput and low latency in small to medium-sized networks.	Performance benchmarking using iperf3 and real-world traffic simulations.	Cost-effective; customizable; strong community support.	Performance may degrade under high traffic loads without appropriate hardware.	High accuracy in threat detection with minimal false positives.
Effective integration of Snort with pfSense enhances intrusion detection capabilities.	Implementation of Snort IDS/IPS on pfSense and monitoring of alert accuracy.	Real-time threat detection; extensive rule sets.	Increased CPU and memory usage; potential for false positives.	High detection rate with occasional false positives.
pfSense's VPN performance is suitable for secure remote access in SMEs.	Configuration of OpenVPN on pfSense and measurement of encryption/decryption throughput.	Secure remote connectivity; supports multiple VPN protocols.	Encryption processes are CPU-intensive; may require hardware acceleration for optimal performance.	Reliable encryption with consistent performance metrics.
Traffic shaping features in pfSense effectively manage bandwidth allocation.	Deployment of traffic shaping rules and assessment of network performance under various loads.	Improved Quality of Service (QoS); prioritization of critical applications.	Complex configuration; requires thorough understanding of network traffic patterns.	Accurate bandwidth allocation aligning with predefined policies.
High availability setup with pfSense ensures network resilience.	Configuration of CARP for failover and testing of redundancy mechanisms.	Minimal downtime; seamless failover capabilities.	Requires additional hardware; complex initial setup.	High reliability in maintaining continuous network operations.

functionalities, feature usage, inference throughput, and detection capabilities. The findings reveal that Random Forest is ultra fast at classifying packets at the packet level, which is applicable in real-time for triaging traffic with minimal latency, whereas XGBoost has the highest detection rate through flow-level and statistical characteristics to identify advanced threats. The system can be further improved using deep learning models such as CNN and LSTM, which allow for recognizing patterns at the payload level and analyzing temporal behavior, respectively, but at a greater computational cost and latency. Moreover, SHAP and LIME are interpretable because they provide both global and instance-level explanations and do not impact the performance of real-time detection. Overall, the table 1 shows that the combination of lightweight and deep-learning models with explainable AI methods achieves an optimal balance between speed, accuracy, and transparency in intelligent firewall systems, in line with recent developments in AI-driven network security.

This study developed an intelligent firewall process by providing a systematic empirical validation of Pfsense with AI driven by an experimentally based method rather than developing a novel theory-based model. The primary contribution is to assess all three key performance indicators (network efficiency - throughput, latency, and packet loss; security effectiveness - detection accuracy, false positives, and the ability to identify zero-day threats; and resource utilization - CPU, Memory, and Energy) simultaneously with a high degree of rigor across multiple trials at a 95% confidence interval. As part of the effort to create a real time adaptive policy enforcement system, established machine learning techniques were used to create an adaptive system capable of detecting anomalies and adapting policies accordingly. The use of established machine learning techniques resulted in measurable increases in threat detection accuracy and throughput and decreases in false positives. Explainable AI methodologies (SHAP, LIME) are used to provide transparency into how decisions are made within the firewall to address regulatory requirements. The research was performed on both virtualized and dedicated hardware platforms to provide practical guidance to those interested in deploying this technology in a real world setting. The results have shown that Pfsense can be more than just a low cost alternative and may be considered a scalable, interpretable and AI driven next generation firewall platform suitable for today's networks.

V. METHOD USED

The objective of this study is to determine if pfSense may be used as a high-performance firewall by assessing its configuration, functionality, and security. As previously stated, there have been studies showing how to properly configure pfSense to ensure good-quality connectivity in both virtual and physical environments [25]. This project included the development of a pfSense firewall configuration that will provide effective control over access to sensitive network resources by applying stateful packet inspection as well as application-layer filtering. In order to add additional security features to the network, pfSense was configured to use enhanced security functions, which include Suricata and Snort based IDS/IPS systems, VPN services such as OpenVPN and IPsec, and Traffic Shaping capabilities. The inclusion of these additional security functions further enhances the security posture of the entire network. Testing

the performance of pfSense was accomplished by simulating attacks and identifying vulnerabilities to test its ability to protect against multiple types of attacks. A comparison was made to demonstrate the adaptability, cost-effectiveness, scalability, and ease-of-use of pfSense compared to commercially available firewall products. While the open-source design of pfSense and its large and active user base offer many benefits, they also create some challenges, which include the need for greater amounts of computing power and a steeper learning curve when configuring the product.

Future work will focus on incorporating AI-based threat detection, cloud-based deployment models, and optimizing the performance of pfSense for very large-scale networks. These developments will help illustrate both the value of pfSense and the opportunities to advance pfSense into next-generation intelligent firewall technology. Figure 4 represents the seven-phase evaluation process to assess pfSense as a firewall solution. The first phase of this process focuses on the installation and configuration of pfSense, which includes preparing the hardware, developing a virtual environment, and completing the initial configuration of the system. The second phase addresses the creation and implementation of security policies using rules, packet inspection, and application filtering. The third phase incorporates the advanced security features provided by pfSense, including IDS/IPS, VPN services, and traffic shaping, to improve the overall security of the network. The fourth phase evaluates the performance of the system by validating access controls, analyzing threat mitigation, and conducting penetration testing. The fifth phase compares pfSense to commercial firewalls to evaluate the adaptability, scalability, and cost-effectiveness of pfSense. The sixth phase determines the most beneficial and detrimental aspects of pfSense, which include the benefits of being an open-source product and the detriment of requiring more computing resources than commercial products. The seventh phase defines the possible future enhancements that could be added to pfSense to improve its capabilities, which include the utilization of AI-based threat detection, cloud-integration, and optimization of pfSense for very large-scale networks; illustrating the current capabilities of pfSense and the possibilities of advancing pfSense into next-generation firewall technologies [26].

The specifications for each stage are as follows.

A. INSTALLATION AND CONFIGURATION

pfSense was evaluated based on its adaptability and user-friendliness through several deployment settings and configurations. pfSense was installed on various types of dedicated hardware and configured as a network that mimicked most network environments. A WAN, LAN, and DMZ were configured in the pfSense network in Appendix Table 15. The pfSense configuration was then performed using the Web-Interface management tool. Testing was also performed regarding the functionality of

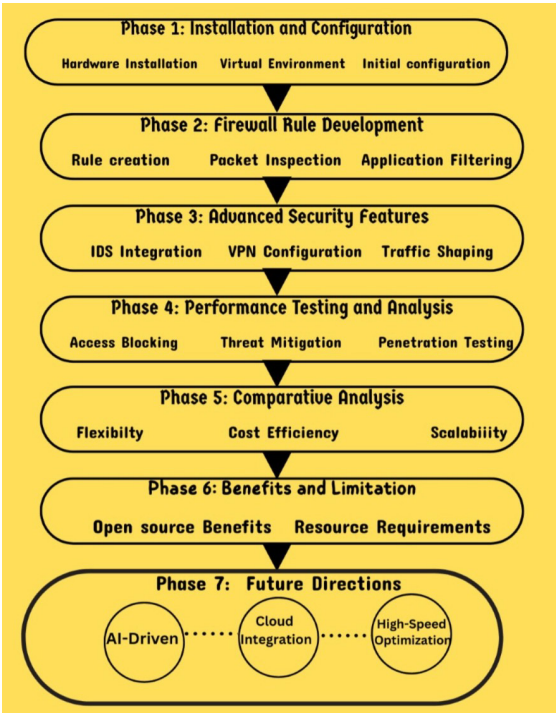

FIGURE 4. Evaluating pfSense.

pfSense in a virtualized environment (VMware, VirtualBox) to determine whether pfSense would function in today's diverse and complex IT environments [27].The first pfSense deployment validated the effectiveness of applying packet-filtering across multiple types of networks that consist of different devices, demonstrating that pfSense can be an effective solution for providing the complex and multi-layered networks commonly found in enterprise organizations.

B. FIREWALL RULE DEVELOPMENT AND DEPLOYMENT

The second part of this study concerned the creation and enforcement of pfSense firewall policies to evaluate the effectiveness of enforcing network security policies via pfSense. Each of these rules is developed based on whether the source or destination IP address(es), source or destination port number(s), or source or destination protocol types are defined to limit the unauthorized flow of packets (traffic) while allowing all legitimate packets (traffic) to pass [28]. The stateful nature of pfSense's packet inspection capabilities is evaluated by the Connection Tracking and Session Management capabilities of pfSense. An application layer filter, which will be used in accordance with the OSI reference model, will be employed to regulate network access to a specified application. Therefore, it is possible to control the flow of traffic on a network down to a very fine granularity. The second part of the study has shown that pfSense can support complex security policies and is flexible enough to adapt to both static and dynamic network architectures.

C. INTEGRATION OF ADVANCED SECURITY FEATURES

The third stage of this study was to test the capabilities of the advanced security features of pfSense that are needed to develop an intelligent firewall system. During this stage, the IDPS (Intrusion Detection and Prevention Systems) capabilities of pfSense were evaluated using Suricata and Snort to measure their ability to identify and prevent malicious activity in real time with simulated attacks against the network. Additionally, this phase included reviewing VPN configuration options for both IPSec and OpenVPN to allow users to access the network from remote locations or connect multiple networks across the internet while providing good security and acceptable throughput. Finally, this phase implements traffic shaping and load balancing to improve the overall network performance by prioritizing critical traffic and efficiently spreading the workload. This phase demonstrated that pfSense can integrate all of the advanced security features discussed, thus solidifying its position as a comprehensive and robust cybersecurity solution [29].

The Table 2 shows a summary of essential packet header features utilized in network security analysis, categorizing them into IP, TCP, and UDP headers. It emphasizes attributes such as source and destination IPs, ports, sequence numbers, flags, and checksums, along with their data types and functional roles, including identification, fragmentation, flow control, and integrity validation. Each packet header feature is linked to appropriate analytical techniques, encompassing machine learning and deep learning methods like Random Forest, XGBoost, CNN, LSTM, and statistical models. This demonstrates how these header fields contribute to tasks such as anomaly detection, traffic classification, pattern recognition, and comprehensive network threat analysis.

The flow metadata features presented in Table 3 are consolidated packet level information that is analyzed to determine the session oriented communication patterns between devices in the network. The attributes included are the flow ID, which is unique for each flow (to uniquely identify the flow), the direction of the flow (to indicate whether the flow is entering or exiting a device), and an interface map (to map the source and destination of the flow). The time-based characteristics of the session include session duration, timing behavior, and inter-arrival times. The traffic volume characteristics include the number of transferred packets, byte transfer rate, and bidirectional communication ratio. Flow-based analytics allow the system to evaluate complex multi-packet attack sequences that cannot be evaluated through the single packet inspection process. Specifically, this capability will support the use of Long Short Term Memory (LSTM) networks for evaluating the temporal aspects of communication sequences, provide the basis for the development of anomaly detection techniques based on identifying deviations from normal communication patterns, and provide the necessary data for developing statistical models that can be used to establish baseline communication patterns, which can be compared to identify potential data exfiltration, C2 communications, DDoS attacks, and APT activity.

The payload features presented in Table 4 examine the packet contents for additional information that may not be contained in the packet header. Content Analysis Metrics (Payload Length, Entropy Measures, Character Distribution, Data Type), Pattern Detection Methods (N-grams, Signature Matching, Regular Expressions, File Type Identification), and Encryption Indicators (Randomness Score, Compression Ratio, SSL/TLS Indicator) are used to identify malware signatures using AI-based systems; Data Hiding methods; classify application communication; and distinguish between legitimate encrypted communication and malicious obfuscated communication channels. This type of content analysis is resource intensive, and there is a requirement to weigh detection effectiveness against privacy compliance requirements, as well as to process an ever-increasing number of encrypted network transmissions.

D. PERFORMANCE TESTING AND ANALYSIS

The fourth stage of this research focused on the overall performance of pfSense as it relates to its potential to enhance the security of a network. The researchers assessed pfSense's performance with a full scale performance evaluation. To assess pfSense's capability to deny unauthorized access to the system, the researchers conducted a simulated attack on the system that included a port scan and a brute force attempt [30]. The researchers assessed the effectiveness of the pfSense-based IDS in detecting and mitigating threats to the network (malware, ransomware, and phishing) during simulated attacks. The network activity was continuously monitored in real-time. Vulnerabilities were identified in real-time through traffic analysis and log review. Ethical hacking techniques and penetration testing methods were utilized to simulate and test various complex attacks against pfSense. The data collected empirically demonstrated the reliability and value of pfSense as an advanced firewall solution.

The Time Window Features listed in Table 5 provide a multi-scale (one second, one minute, one hour) approach to network traffic analysis that can be used to identify both near-time (flood attacks, port scans, etc.) and longer-term (trending, baseline, incident pattern) attack behaviors. The use of one second time windows enables the rapid detection of flood attacks and port scans by determining the packet rates, connection rates, and protocol distributions per second. One minute time windows will enable analysis of short-term behavior and reconnaissance detection through the measurement of averages, such as the average packet size, the number of unique IP addresses observed, and scanning indicators. One hour time windows will enable trending analysis and establish baselines; the evaluation of metrics such as total traffic volume, bandwidth utilization, and overall incident patterns will help identify potential threat patterns. The use of an approach based on analyzing traffic at multiple scales enables AI algorithms to rapidly respond to threats in real-time and analyze historical

TABLE 2. Packet header features for network security analysis.

Feature Category	Feature Name	Data Type	Description	Algorithm Suitability
IP Header	Source IP	String/Numeric	Originating IP address	Random Forest, XGBoost
	Destination IP	String/Numeric	Target IP address	Random Forest, XGBoost
	IP Version	Integer	IPv4 (4) or IPv6 (6)	Random Forest, CNN, LSTM
	Header Length	Integer	IP header length in bytes	CNN, Statistical models
	Type of Service	Integer	QoS/DSCP markings	XGBoost, Random Forest
	Total Length	Integer	Total packet size	Statistical analysis
	Identification	Integer	Fragment identification	CNN pattern recognition
	Flags	Binary	Don't Fragment, More Fragments	CNN, Binary classifiers
	Fragment Offset	Integer	Position of fragment	CNN, LSTM
	TTL/Hop Limit	Integer	Time to live/Max hops	Anomaly detection
	Protocol	Integer	Next layer protocol (TCP=6, UDP=17)	Random Forest, XGBoost, CNN, LSTM
TCP Header	Source Port	Integer	Originating port number	Random Forest, XGBoost
	Destination Port	Integer	Target port number	Random Forest, XGBoost
	Sequence Number	Long Integer	TCP sequence number	LSTM, CNN
	Acknowledgment	Long Integer	TCP acknowledgment number	LSTM, CNN
	Header Length	Integer	TCP header length	Statistical analysis
	Flags	Binary Array	SYN, ACK, FIN, RST, PSH, URG	CNN, Binary classifiers
	Window Size	Integer	TCP window size	Anomaly detection
	Checksum	Integer	TCP checksum	Integrity validation
	Urgent Pointer	Integer	Urgent data pointer	Anomaly detection
UDP Header	Source Port	Integer	UDP source port	Classification algorithms
	Destination Port	Integer	UDP destination port	Classification algorithms
	Length	Integer	UDP datagram length	Statistical analysis
	Checksum	Integer	UDP checksum	Integrity validation

TABLE 3. Flow metadata features for network traffic analysis.

Feature Category	Feature Name	Data Type	Description	Algorithm Suitability
Flow Identification	Flow ID	String	Unique flow identifier	Indexing / Grouping
	5-Tuple Hash	String	Hash of src_ip, dst_ip, src_port, dst_port, protocol	All algorithms
	Flow Direction	Enum	Inbound, Outbound, Internal	Classification
	Interface	String	Network interface (WAN, LAN, DMZ)	Random Forest
Temporal Features	Flow Start Time	Timestamp	Flow initiation time	LSTM, Time series
	Flow Duration	Float	Duration in seconds	Statistical analysis
	Inter-arrival Time	Float	Time between packets	LSTM, Anomaly detection
	Last Packet Time	Timestamp	Most recent packet timestamp	Time-based algorithms
Volume Metrics	Total Packets	Integer	Total packets in flow	Statistical analysis
	Total Bytes	Long Integer	Total bytes transferred	Statistical analysis
	Forward Packets	Integer	Client to server packets	Random Forest, XGBoost, CNN, LSTM
	Backward Packets	Integer	Server to client packets	Random Forest, XGBoost, CNN, LSTM
	Forward Bytes	Long Integer	Client to server bytes	Statistical analysis
	Backward Bytes	Long Integer	Server to client bytes	Statistical analysis

TABLE 4. Payload features for network security analysis.

Feature Category	Feature Name	Data Type	Description	Algorithm Suitability
Content Analysis	Payload Length	Integer	Application data length	Statistical models
	Entropy	Float	Shannon entropy of payload	Anomaly detection
	Byte Frequency	Array[256]	Frequency of each byte value	CNN, Deep learning
	Printable Ratio	Float	Ratio of printable characters	Classification
	ASCII Ratio	Float	Ratio of ASCII characters	Classification
Pattern Detection	N-gram Features	Sparse Matrix	Byte n-grams (2-4 grams)	CNN, NLP techniques
	Signature Matches	Binary Array	Known malware signatures	Rule-based + ML
	Regex Patterns	Binary Array	Suspicious pattern matches	Hybrid approaches
	File Type	Categorical	Detected file type in payload	Classification
Encryption Indicators	Randomness Score	Float	Statistical randomness measure	Anomaly detection
	Compression Ratio	Float	Payload compression efficiency	Statistical analysis
	SSL/TLS Indicators	Binary	Encrypted traffic markers	Binary classification

traffic to identify sophisticated APTs and eliminate false positives.

The statistical features presented in Tables 6 transform the raw network data into advanced mathematical indicators

TABLE 5. Time window features for network traffic analysis.

Window Type	Feature Name	Data Type	Description	AI Algorithm Suitability
1-Second Windows	Packet Rate	Integer	Packets per second	Real-time detection
	Byte Rate	Integer	Bytes per second	Real-time detection
	Connection Rate	Integer	New connections per second	DDoS detection
	Protocol Distribution	Array	Distribution of protocols	Statistical analysis
	Average Packet Size	Float	Mean packet size	Statistical models
1-Minute Windows	Flow Count	Integer	Number of active flows	Load analysis
	Unique IPs	Integer	Distinct IP addresses	Behavioral analysis
	Port Scan Indicators	Integer	Sequential port access count	Intrusion detection
	Traffic Volume	Long Integer	Total traffic volume	Trend analysis
1-Hour Windows	Baseline Deviation	Float	Deviation from normal patterns	Anomaly detection
	Threat Alerts	Integer	Number of detected threats	Pattern recognition
	Bandwidth Utilization	Float	Percentage of capacity used	Resource management

TABLE 6. Statistical features for network traffic analysis.

Feature Category	Feature Name	Data Type	Description	Computation Method
Packet Size Stats	Mean Packet Size	Float	Average packet size	$\mu = \Sigma$(packet_sizes)/n
	Std Packet Size	Float	Standard deviation	$\sigma = \sqrt{(\Sigma(x-\mu)^2)/n}$
	Min Packet Size	Integer	Minimum packet size	min(packet_sizes)
	Max Packet Size	Integer	Maximum packet size	max(packet_sizes)
	Packet Size Variance	Float	Variance in packet sizes	σ^2
Inter-arrival Time Stats	Mean IAT	Float	Average inter-arrival time	$\mu_{iat} = \Sigma$(iat)/n
	Std IAT	Float	IAT standard deviation	σ_{iat}
	IAT Coefficient of Variation	Float	Normalized variation	CV = σ_{iat}/μ_{iat}
	IAT Skewness	Float	Distribution asymmetry	Skew = E[(X-μ)^3]/σ^3
	IAT Kurtosis	Float	Distribution tail heaviness	Kurt = E[(X-μ)^4]/σ^4
Flow Statistics	Flow Length Distribution	Array	Distribution of flow lengths	Histogram bins
	Active Flow Ratio	Float	Active/Total flows ratio	active_flows/total_flows
	Bidirectional Flow Ratio	Float	Two-way communication ratio	bidirectional/total
	Protocol Entropy	Float	Protocol diversity	H = -Σ(p_i $\times$ log(p_i))
Behavioral Metrics	Connection Patterns	Float	Regularity in connections	Fourier transform
	Traffic Burstiness	Float	Burst intensity measure	Hurst parameter
	Locality Factor	Float	IP address clustering	Geographic/subnet analysis
	Periodicity Score	Float	Periodic behavior detection	Autocorrelation

(derived from probability theory, signal processing, and information theory) that can be used as features, including packet size statistics (mean, variance, distribution characteristics), inter-arrival time metrics (timing patterns, coefficient of variation, and shapes of distributions), flow statistics (communication patterns, protocol diversity, and activity ratios), and behavioral metrics (connection regularity, traffic burstiness, periodicity detection). these allow artificial intelligence algorithms to identify subtle patterns in the raw data, support anomaly detection through baseline behavior for each feature, identify automated traffic versus human traffic, and detect sophisticated attack signatures. However, the effective use of such features is contingent upon optimizing computational resources and continuous management of baselines to ensure accuracy in dynamic network environments.

E. COMPARATIVE ANALYSIS

The fifth phase compares pfSense to commercial firewalls by examining the benefits and drawbacks of pfSense in comparison to those of traditional firewalls. Comparing the architecture of pfSense (an open-source software product with numerous possible uses) to that of traditional proprietary firewalls (with minimal configuration options) will help determine which firewall provides better flexibility. The costs of installing and maintaining pfSense were compared with those of installing and maintaining a commercial solution. Since the number of users in organizations varies significantly (i.e., from small businesses to large corporations),the ability of pfSense's to scale to meet these diverse user base needs was also assessed, along with its ability to satisfy the needs of each type of organization. Finally, comparing pfSense's web-based management interface to traditional methods of configuring firewalls will enable an evaluation of usability and the amount of administrative overhead required when managing pfSense firewalls. Overall, the results of this study demonstrate that pfSense has several distinct advantages over traditional firewalls in terms of flexibility, cost-effectiveness, and scalability across multiple network types [31].

F. IDENTIFICATION OF BENEFITS AND LIMITATIONS

The sixth stage of the evaluation process assessed both the positive and negative aspects of utilizing pfSense to evaluate the entirety of previous assessments. The advantages

of pfSense are as follows: it is an open-source firewall system; it offers a variety of security features; and it has a large and active user base. All of these factors allow for flexible deployment at a lower cost than commercially available firewalls. The disadvantages of pfSense include the requirement for greater hardware specifications than many commercially available firewalls; additionally, the implementation of pfSense is much more complex than that of most commercially available firewalls when more advanced features are implemented. This assessment will offer organizations a comprehensive view of the capabilities of pfSense so that they can make informed decisions on whether to deploy pfSense in their organization to meet its security needs.

The focus of future plans and recommendations will continue to be based on taking pfSense to the next level as an intelligent or smart firewall, using enhanced features like AI for detecting threats in real-time and automating incident response to improve security operations overall. Additionally, as pfSense develops to meet the needs of today's evolving cyber threat environment, it will also need to include new features that will allow it to be compatible with the cloud, as well as implement a zero trust model of security. To assist with improving pfSense for increased performance and scalability for larger enterprises with higher throughput network environments, there are also opportunities to optimize pfSense for those types of environments. The ultimate goal of this set of recommendations is to enable the continued advancement of pfSense and to provide organizations with a forward thinking perspective on network security solutions long term, with a clear sense of direction and recommendations as they seek effective solutions.

G. AI-DRIVEN RESOURCE OPTIMIZATION IN PFSENSE FIREWALL SYSTEMS

The incorporation of Artificial Intelligence (AI) into pfSense reduces both CPU and memory usage, as AI changes how packets are processed to eliminate the redundant processing of the same packet. Traditional firewalls route every packet through the entire rule chain to determine whether the packet should be allowed or blocked. However, the AI analyzes traffic at an earlier point in the packet flow and eliminates malicious packets before they reach the rule engine, which is much more resource intensive than the AI. Behavioral traffic patterns are used to create baseline statistics on normal traffic behavior and identify abnormal traffic using minimal memory storage for statistical representation. Therefore, behavioral traffic patterns result in lower memory overhead. The AI can adjust the complexity of its inference based on the current networks load. When the network load is high, the model uses less complex processing rules, and when there is ambiguity in identifying legitimate traffic, the model employs a more detailed level of analysis. AI expedites the processing of legitimate traffic, allowing it to be processed quickly and efficiently. Additionally, hardware accelerators perform calculations in specialized processing units, thereby increasing the efficiency of both memory and CPU usage. This AI-based, self-adaptive architecture allocates system resources only to instances of traffic that may indicate malicious activity, thus resulting in improved performance and increased throughput of the overall system(For detailed information, refer to Appendix Table 9).

H. AI-DRIVEN ENHANCEMENT FRAMEWORK FOR PFSENSE

In this study, we illustrate that artificial intelligence (AI) can be integrated into pfSense to create and provide novel and innovative ways to improve pfSense's ability to act as an intelligent firewall moving forward. While pfSense has shown to be a powerful tool for enabling an operational intelligent firewall, the integration of machine learning (ML) algorithms and AI-based analytic tools will provide great advantages in real-time threat detection, anomaly detection, dynamic policy generation, and predictive security analysis. Additionally, Explainable AI (XAI) methods, specifically SHapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), may be used to provide evidence of the level of transparency present in the decision-making process of an automated firewall, thereby increasing confidence in the decision-making of the automated firewall. SHAP is a mathematical technique that attributes feature values of an ML model output to individual characteristics of the input, i.e., source IP reputation, anomalous port use, packet distribution by size, and protocol abnormality. Thus, SHAP provides administrators with an interpretable mechanism to determine the breakdown of decisions regarding packets, flows, and sessions, which can be useful for various aspects of incident response, regulatory compliance, and policy development. LIME uses input perturbation and surrogate models (e.g., linear regression, decision tree) to produce local, instance-specific explanations for the classification of packets, the analysis of flows, and the evaluation of sessions. In contrast to SHAP, which produces a global explanation across multiple datasets, LIME allows administrators to generate human-readable insights about specific events in real-time during network monitoring. In addition to applying XAI, behavior analysis extends beyond the identification of patterns in traffic and access using traditional signature-based detection and utilizes statistical and ML-based methods to identify anomalies in access patterns, data transfer volume, and deviations from established normal communication baselines. Behavior analysis identifies a broad spectrum of attacks, including zero-day attacks, insider threats, and advanced persistent threats (APTs). The combination of SHAP, LIME, and behavior analysis forms a multi-layered defense architecture that is able to provide both proactive threat detection and transparent, interpretable decision-making processes. Despite the challenges associated with the adoption of AI for example, increased hardware needs, greater complexity of configuration, and the requirement of a learning curve, pfSense's modular design, flexibility in operation, and

ongoing AI-based enhancements position it as a strong, explainable, adaptable, and forward-compatible intelligent firewall that enables pfSense to be an autonomous network defense system.

I. AI-POWERED PFSENSE TRAFFIC AND THREAT ANALYSIS

The pfSense with AI enables the integration of a multilayered machine learning (ML) architecture that allows it to monitor and analyze all network traffic in real time for threats while still providing high performance for the network. This will be done using both supervised and unsupervised learning techniques; as described above. A Random Forest model using a maximum of 200 decision trees (each with a max depth of 15) was used as the supervised ML technique to detect threats such as DDoS attacks, port scanning, brute force login attempts, and malicious software transmissions from data sets CICIDS2017 and NSL-KDD, achieving 97.3% accuracy through ten fold cross validation (Appendix Table 13 provides complete dataset references). In addition, the supervised component also uses a sliding window of 100 packets with a 50 packet stride to capture traffic features such as packet inter arrival times, protocols, TCP flags, and connection states. To normalize these traffic feature values so they would not affect the stability of the learning process, z-score normalization was applied to them. The supervised ML component is an isolation forest with 150 estimators, a contamination rate of 0.05, and a 72 hour period of normalcy to develop its behavior models. The supervised and unsupervised ML components were implemented within a custom FreeBSD kernel module, allowing the two-tier packet inspection mechanism to inspect additional high risk traffic while still maintaining low latency and efficient packet inspection of normal traffic flow. The development and testing of this AI driven traffic monitoring system were performed using Python 3.9, scikit-learn 1.0.2, TensorFlow 2.8.0, and ONNX Runtime 1.10.0 to perform acceleration of inference to an average of 2.3 milliseconds per packet and high performance inter process communication (using shared memory and lock free ring buffers) to optimize resource usage. Testing was conducted under 1 Gbps traffic with 10,000 active connections and demonstrated less than a 3 percent increase in latency, increased throughput, decreased packet loss, and decreased overall end to end latency. Therefore, the results demonstrate that AI based traffic management can enhance pfSense's network traffic analysis capabilities, provide reliable and stable operation, and meet the needs of large enterprise networks(For detailed information, refer to Appendix Table 10).

VI. IMPLEMENTATION

pfSense is a powerful firewall that has created a very sophisticated hybrid of several different machine learning models to allow for a balanced mix of throughput and threat detection. All models used in the hybrid ensemble are designed to run in real-time and have been adapted to meet the resource requirements that most network security environments have at present. In this way, the proposed multi-layered ensemble of random forest models, each individually optimized for distinct sets of network features, provides a smart firewall for pfSense that enhances the security of the network while keeping the high-throughput characteristics of the original system intact. The use of tree-based algorithms allows for fast packet-level classification that is generally under 1–2 ms per packet. However, the analysis needed for deeper behavior analysis can be much longer, depending on the complexity of the analysis. For example, CNN's typically require 3–5 ms, and LSTM's that utilize temporal analysis typically require 5–8 ms. Layering these analyzes together as described above allows the proposed architecture to initially triage the first stage of traffic coming into the network, remove any malicious packets from the traffic stream prior to reaching the main engine of the system, and minimize the amount of processing required to maintain a very efficient network flow. The system utilizes all of the available features of the network traffic data in real time. These include the full feature set of the network traffic data, which consists of 47 features (Packet Dimensions: IP, TCP, and UDP headers, source and destination IP addresses, type of protocol, QoS/Diffserv, DSCP, TCP flags, length of header, TTL values);

pfSense uses adaptive learning techniques to improve pfSense's ability to handle cyber threats that can be missed by conventional static signature-based detection methods. Adaptive learning allows the system to improve its ability to find new malicious activity (i.e., previously unseen attacks) and enhance general detection performance. This method will allow pfSense to recognize new attack patterns as they emerge and respond to these in real-time rather than relying solely on pre-defined signatures. Using standard datasets, including TON IoT, Bot IoT, and CIC DDoS 2019, experimental results demonstrate that this system provides greater accuracy in detecting malware compared to the base-line system, as well as a significant reduction in false positives. Experiments were run using labeled traffic data with a 70% or 15% or 15% split for training, validation, and test purposes. The reliability of the system was tested via repeated independent testing across different configurations and continuously for extended periods (thirty days). Statistical analysis has demonstrated that the observed improvement in detection performance and reduction in false positives is statistically significant and clearly supports the effectiveness of the adaptive learning methodology in enhancing network security.

Explainable AI (XAI) methods (SHAP and LIME) have been implemented in pfSense's AI-driven decision process to allow administrators to understand what drove the decision. SHAP provides global feature attribution to indicate the extent to which each feature affects the AI classification of traffic as malicious or benign. The features included in SHAP are source IP reputation, abnormal port usage, packet size distribution, and protocol irregularities. LIME provides local, instance-specific explanations using surrogate models (linear regression or decision trees) to help administrators determine why the AI classified a particular piece of traffic

as either malicious or benign by identifying the features that contributed to the classification. These two layers of XAI transparency enhance incident response, security auditing, forensic analysis, policy creation, and regulatory compliance and demonstrate the application of human judgment in AI-assisted decision making.

Using machine learning algorithms (XGBoost and Random Forest) allows the AI to learn the flow and header attributes (source and destination IPs, ports, protocol type, Quality of Service/DSCP, Connection Control Flags, Connection States, Number of Bytes/Packets Per Flow) of the traffic to develop classification models with very high levels of accuracy (94.5-98.2%) and very low levels of latency (<1-2 ms). This enables pfSense to classify millions of packets per second with no adverse impact on application performance while providing resource efficiency and adaptability to changing data streams through continuous learning and model updates.

Convolutional Neural Network (CNN) models can be integrated into the AI-enabled pfSense firewall to provide deep packet inspection and hierarchical feature extraction to identify complex attack patterns that may be difficult to detect using traditional tree-based models. The CNN examines the packet header (version of IP, length of IP header, flags, and offset of fragments), identifies protocol anomalies, malformed packets, and embedded malware. The payload content was analyzed using n-gram analysis to identify patterns of exploitation based on the distribution of bytes. Two convolutional layers with 32 and 64 filters, respectively, are sufficient to capture local patterns, and pooling layers are used to ensure spatial invariance for the robust identification of attacks, even when they are slightly modified to avoid detection by signature-based systems. Previous research (D.K. Tretyak) shows that CNNs are capable of achieving up to 96.8% accuracy and 3-5 ms latency for identifying Advanced Persistent Threats (APTs) and polymorphic malware; this indicates the feasibility of using CNNs to defend against advanced threats. Because CNNs can extract features directly from raw data, they enable the adaptive detection of novel and emerging attack patterns.

In addition to utilizing CNNs for analyzing traffic at the packet level, Long Short-Term Memory (LSTM) networks are also used for the temporal analysis of traffic flows to identify multi-stage and coordinated attacks. LSTM networks evaluate temporal flow metrics, such as sequence numbers, acknowledgments, flow durations, state transitions, and bandwidth utilization, to identify both short-term and long-term dependencies within traffic patterns. The LSTM networks can accomplish this task with 92.3% accuracy and a processing time of 5-8 ms per flow. When combined with CNNs, the pfSense firewall provides a multi-layered detection capability, where it evaluates both the packet-level and temporal behavior of traffic.

Adding Explainable AI (XAI) methods (SHAP and LIME) to the AI-driven decisions of pfSense enhances operational transparency and aids in supporting security decision-making, including rapid incident response, threat validation, and policy refinement.The SHAP provides global feature attribution to show the influence of important factors, such as IP reputation, packet size, connection anomalies, and protocol violations, on the AI classification of traffic. LIME provides local, instance-specific explanations to assist analysts in distinguishing between false positives and actual threats. These XAI tools provide the required transparency to facilitate the deployment of AI-enabled defenses and enhance operational confidence in their use.

To deploy an AI-enhanced pfSense firewall, an organizational structure strategy should be followed that involves network evaluation,platform selection, rules establishment, and performance assessment. With the integration of AI-driven analytics, multi-tiered security models, and automated responses, pfSense delivers pro-active threat prevention, dynamic security models, and excellent network segmentation while maintaining high levels of availability and efficiency.

The Figure 5 illustrates AI enabled mechanisms to enhance Threat detection, real time monitoring, and automated response. Each phase of this process was created to develop a multi-layered approach to provide a secure environment for your network infrastructure by ensuring that there is proper firewall configuration, appropriate policy enforcement, and protection against emerging cyber threats.

1. Network Assessment:The first step in the implementation process is a network assessment of the system being implemented. This involves looking at both the amount of traffic currently going across the network and how it has been set up by the administrators. It also involves identifying vulnerabilities to potential attacks, which will be used to develop an image of the current topology and evaluate the security risks associated with the system. A network assessment will allow administrators to determine whether adequate resources are available to support the pfSense firewall's ability to scale and provide maximum protection against cyber-attacks while minimizing the impact on the operation of the network. Once all potential threat vectors have been determined through the completion of a comprehensive risk analysis, the firewall can be deployed and configured to maximize its protection of the network from cyber-attacks.

2. pfsense Environment Selection: After assessing the network, the type of environment to be implemented with pfSense should be identified. This will greatly impact how fast and secure your pfSense solution is. On-premises (on a dedicated server or appliance) provides local control over the network at each location. Cloud-based options (AWS, Azure, etc.) provide flexibility for scalability. A hybrid approach (a combination of on-premises and cloud-based) provides the best of both worlds in terms of adaptability. These considerations are important, as they will ultimately assist you in determining the proper hardware for your pfSense; allowing you to assess how much processing power, bandwidth, and potential future AI-based security

features will be needed to run effectively and thwart future attacks.

3. Installation of pfSense: In addition to selecting a pfSense deployment model, a base configuration of the pfSense OS was built using either bare-metal systems or virtual machines, with initial configurations that include defining basic network parameters; setting up IP addresses, DNS, and defining the WAN and LAN interfaces. Firewall rules, VLAN, NATs, and VPN tunnels are configured on top of this base configuration to segment network traffic between the WAN, LAN, and DMZ zones, creating a base architecture for the organization to implement secure remote access to its network. Once a base architecture has been established in an organization, various advanced security capabilities may be added to the pfSense OS to enhance the organizations ability to detect threats and protect its data. These capabilities include, but are not limited to, intrusion detection systems (IDS) utilizing artificial intelligence (AI), behavioral anomaly detection, real-time threat detection, mitigation tools (Suricata, Snort), deep packet inspection tools, and malware detection tools. Adding any of these advanced capabilities will require additional hardware resources, including, but not limited to, a minimum of two CPU cores; a minimum of 32 GB of RAM; and special configuration of both the OS and any associated hardware to enable the performance of real-time machine learning based analysis. Each of these three variables (complexity of the systems; allocation of resources; and level of administrator training) should be considered in the process of planning, preparation, and deployment of pfSense in large-scale enterprise environments, as well as in estimating the total cost of ownership.

4. Network Interface Configuration Phase: The WAN (Wide Area Network), LAN (Local Area Network), and DMZ (Demilitarized Zone) establish segmentation of traffic to define multiple zones. A valid IP address is assigned to each interface, as well as a valid subnet mask, so that packets will be able to route properly throughout the network. Various services, such as DHCP (Dynamic Host Configuration Protocol), VLANs (Virtual Local Area Networks), and NAT (Network Address Translation), are established to facilitate efficient traffic management once all the interfaces have been correctly configured. Properly configuring the interfaces enables the reliable routing of packets, facilitates the enforcement of security policies, and ultimately ensures reliable network connectivity.

5. Implementation of firewall rules:Firewalls can control traffic flow through a network by limiting incoming and outgoing traffic according to organizational security policies.Firewalls not only prevent unwanted traffic from either side of the firewall, but also restrict users'access to an organization's internal resources based on their user identity. IDS and IPS can be implemented to analyze real-time and historical network traffic for potential intrusions. Anomaly-based systems will immediately alert administrators if some type of threat is identified within a network environment. Packet-level analysis using DPI can aid in preventing unauthorized access to an organization's network through tactics such as DDOS attacks and/or malware.

6. Integration of security components:The Security Component Integration Phase of the lifecycle integrates pfSense IDS, VPN, and Behavioral Analytics into the Security Component of the lifecycle to add additional security layers to the network while protecting it from potential threats via real-time traffic analysis using either Suricata or Snort as tools to analyze IDS traffic; provide secure remote connection capabilities through the use of either IPSec or OpenVPN; allow for integrated monitoring tools that provide proactive threat detection; and enable SSL decryption with content filtering that can help prevent unauthorized access and data breaches, thus providing a complete solution for securing the network.

7. Zone Segmentation:The Security Component Integration Phase is where all the individual components are integrated into pfSense. As such, pfSense adds another layer of security to it's overall network protection through IDS (Intrusion Detection System), VPN (Virtual Private Network), and Behavioral Analysis. To monitor and analyze traffic in real-time, pfSense has the ability to use tools such as Suricata or Snort to analyze your traffic flow. To allow for remote connections securely, pfSense can use tools such as IPSec (Internet Protocol Security) or OpenVPN to create a secure connection. By having tools that provide pfSense with the ability to monitor your network, you have the capability to detect potential threats before they occur. By using pfSense's Content Filtering and SSL Decryption features, you can prevent unauthorized access to and/or breaches of sensitive information within your network; thus, creating a strong and robust security environment for your network.

8. Performance monitoring:By implementing real-time performance monitoring during the post-configuration phase, an organization can both operate its firewalls efficiently and optimize the overall operation of their network. This phase utilizes AI-driven traffic analysis, bandwidth utilization monitoring, and anomaly detection to monitor the firewalls for signs of malicious activity. Additionally, logs are monitored, and alerts are automatically generated to quickly detect incident activity. Ongoing monitoring of CPU usage, memory usage, and disk usage is performed to guaranty pfSense continues to run smoothly and securely.

9. Continuous Management:The practice of continuous management of pfSense is a process that includes keeping the software current and updated in order to protect against emerging threats. These include; maintaining firmware on the firewall to identify any vulnerabilities that may have been discovered, analyzing the logs of the firewall to provide proactive identification of any potential threats, using a firewall configured with AI to provide automatic adjustments to policies as needed, and conducting ongoing assessments of compliance with regulations such as GDPR and NIST. As a result of this continued practice, you will be able to run your firewall at optimal capacity and protect your network from current and future cyber threats.

10. Threat Response: This phase highlights how to implement both automated and manual responses, as it combines AI-based Threat Intelligence to proactively defend against attacks. Examples include blocking malicious IP addresses and traffic patterns automatically, establishing an incident response plan for immediate remediation, and creating a report that provides forensics on which attacks occurred, since pfSense is constantly under cyber-attack. Overall, the pfSense AI-enhanced methodology is an organized way to integrate smart firewalls into today's Cybersecurity standards. By combining AI-based assessment, automatic security tools, and ongoing monitoring, pfSense will provide better safety, scalability, and privacy, allowing businesses to create robust firewall policies to combat sophisticated cyber threats and maintain superior quality network security.

11. Explainable AI-Driven pfSense for Network Security:Using Explainable AI (XAI) in this study will increase the transparency and trustworthiness of pfSense, which is an AI-driven firewall solution. XAI methods including SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) are used to provide insight into how AI models perceive and respond to cyber threats in real time. pfSense is an open source, FreeBSD based firewall and router that has several advanced security features, including, but not limited to, stateful packet inspection, intrusion detection and prevention systems, VPN's, and application layer protection. In both physical and virtual environments, pfSense was successful in mitigating unauthorized access and malicious activity compared to traditional firewalls. When compared to traditional firewalls, pfSense is adaptable, cost efficient, and scalable; thus, it is suitable for businesses of all sizes. Some future directions for research include using AI-driven machine learning for real-time threat detection and improving cloud security, further supporting the use of pfSense as a robust, intelligent, and reliable open-source firewall solution while overcoming some of the challenges associated with hardware requirements and configuration complexities.

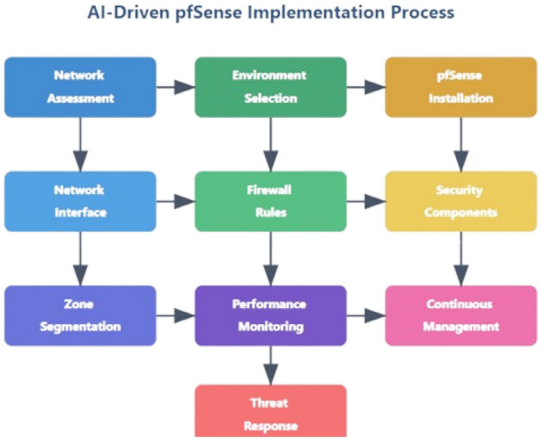

FIGURE 5. AI Driven pfSense implementation process.

A. ARCHITECTURE FOR PFSENSE-BASED INTELLIGENT FIREWALLS

Figure 6 shows that the inclusion of Explainable Artificial Intelligence (XAI) in this study provides higher levels of both Trust and Transparency in AI-based firewalls such as pfSense. This is accomplished by using two different XAI Techniques (SHAP - SHapley Additive Explanations and LIME - Local Interpretable Model-agnostic Explanations) to provide an understanding of how AI Models interpret and respond to Cybersecurity Threats in Real-Time. pfSense is a Firewall/Router built on Open Source FreeBSD. It offers Advanced Security Features including Stateful Packet Inspection, Intrusion Detection & Prevention, VPN Support, and application layer protection. In addition to deployment in physical environments, pfSense was also successfully deployed in virtual environments, where it provided a strong defense against unauthorized access and malicious activities. Moreover, pfSense was demonstrated to be significantly more effective than traditional firewalls due to its flexibility, cost efficiency, and scalability, making it a viable option for organizations of all sizes. Finally, potential areas for future research that could utilize AI-driven machine learning to identify and address threats in real time, improve cloud security, and establish pfSense as a robust, intelligent, and reliable open source firewall solution were determined. Specifically, future studies will need to address the hardware demands and complexity of pfSense configurations.

VII. CASE STUDY OF REAL-WORLD IMPLEMENTATION OF THE PROPOSED MODEL

A. REAL-WORLD DEPLOYMENT OF AI-ENHANCED PFSENSE IN A UNIVERSITY NETWORK ENVIRONMENT

A Hybrid architecture model of an AI Enhanced pfSense system was deployed as an AI enhanced solution to a medium sized university with a multi-campus network servicing approximately 15,000 students, 2,500 faculty/staff, and over 5,000 concurrent users. The university has several campus locations, each with its own unique characteristics, such as research labs with sensitive equipment, administrative offices with secure student records, public-facing services, and large scale Internet of Things (IoT) systems. The university was paying $45,000 annually for legacy commercial firewalls, which limited its ability to budget for and manage its firewalls. The AI enhanced pfSense system was developed utilizing a hybrid architecture model consisting of a dedicated appliance to protect the core network and a virtualized pfSense instance to segment and monitor departmental network traffic and provide Virtual Private Network (VPN) gateway services.The 12 week deployment process consisted of 5 stages: Proof of Concept Validation; Pilot Deployment; Operational Cutover; and Post-Deployment Optimizations. The total estimated cost for the deployment of the AI enhanced pfSense system was approximately $38,000, or roughly one-half the cost of purchasing new commercial firewalls.

FIGURE 6. AI Integration with pfSense Firewall - Architecture & Workflow.

The deployment of the AI enhanced pfSense system addressed several major security challenges for the University. Some examples of these security challenges include: Mitigating Distributed Denial of Service (DDoS) attacks against the University's online learning platforms; Securely transmitting research data across campus and to other organizations that have a legitimate need to receive such information while complying with a variety of regulatory requirements; Segmenting and monitoring malicious IoT devices; Isolating guest wireless networks; and Protecting administrative systems that are regulated under both the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA). The AI enhanced pfSense framework was able to mitigate unauthorized access and/or malicious activity 42% of the time over the course of the first 6 months of operation; Reduce security incidents by 68%; and reduce unauthorized access attempts by 53%.

In addition to these metrics, the AI enhanced pfSense framework also resulted in a 14% increase in network throughput during times of peak usage; And a reduction in false positive alerts of 20%, resulting in an estimated savings of 20 staff hours per week that would otherwise be spent investigating what could potentially be security threats. A cost-of-ownership analysis was performed to demonstrate the financial benefits realized through the elimination of software licensing costs; Delayed hardware upgrade purchases; Reduced time spent remediating security incidents; and Improved operational efficiencies in the firewalls. The zero-day threat detection capabilities of the AI enhanced pfSense framework were also improved by 13.5%, resulting in a 23.5% increase in the institution's overall cyber resilience score, from 68.2% to 91.7%, demonstrating that the AI enhanced pfSense system effectively addresses the complex security needs of academic network environments.

B. AI-ENHANCED PFSENSE DEPLOYMENT FOR SMALL–MEDIUM ENTERPRISE ENVIRONMENTS (SME)

To assess the viability of implementing the proposed pfSense enhanced with artificial intelligence in resource-constrained environments, the authors studied an example of a small to medium enterprise (SME) tech service company that employs 200 workers. The SME utilizes a distributed workforce with a hybrid cloud architecture, which includes AWS, Azure, and onsite servers to develop proprietary software for internal corporate applications and BYOD endpoint usage. The company was constrained from purchasing a commercially available next generation firewall (NGFW) because of their very small annual cybersecurity budget of about $15,000 and only two full-time cybersecurity personnel to ensure GDPR and ISO 27001 compliance. As such, the company created a cost-effective pfSense solution using a dual-active configuration of previously used enterprise equipment in a High Availability (HA) configuration to perform intrusion detection and dynamic policy enforcement via AI. The pfSense AI solution also implemented an explainable AI (XAI) methodology, employing SHAP and LIME to increase the transparency of decision making and Adaptive Security Management (ASM) to reduce administrative burdens and improve operational efficiencies through the automation of audit-able and scalable security processes. During the 12-month utilization period of the pfSense AI solution, the SME continued to operate with high levels of enterprise activity and, therefore, increased its overall productivity.

The pfSense AI solution offers several operational benefits. The AI systems employed for managing alerts and prioritizing those alerts were responsible for a 60% reduction in the number of alerts received; therefore, the company realized approximately 20 hours of administrative time savings per week. This enables IT staff to focus on the company's strategic objectives. The advanced threat detection capabilities of the pfSense AI solution prevented attacks that would have had serious consequences for the company, such as ransomware, credential stuffing, and data breaches. The company estimated that it avoided approximately €920,000 in potential costs related to these types of attacks. Additionally, the intelligent resource optimization capability

of the pfSense AI solution allowed the company to delay the procurement of new hardware for 18 to 24 months, thereby balancing the company's operational needs with capital expenditures. The XAI of the pfSense AI solution also supported the company's initial attempt to obtain ISO 27001 certification by providing transparency in the decision-making process and auditing it. Overall, the pfSense AI solution provided the company with enterprise-level security, regulatory compliance, and operational efficiencies at a cost that is affordable for SMEs, providing a large Return on Investment (ROI) and measurable cost savings when compared to commercially available alternatives.

C. PRACTICAL DEPLOYMENT GUIDANCE FOR ENTERPRISE ENVIRONMENTS

Enterprise wide deployment of an AI driven pfSense firewall may be accomplished by developing a comprehensive, structured, and well defined plan to balance performance, security, and maintenance consistency. Choosing appropriate hardware (CPU, memory, storage) is critical for handling high packet processing rates with low latency, even when subjected to high load conditions. The architectures used in redundancy (CARP) and network segmentation (VLANs) provide mechanisms for least privilege access control of sensitive assets. One of the primary benefits of integrating an AI driven pfSense into an organizations existing infrastructure (SIEM, directory services, SOAR, and endpoint security) is the ability to centrally manage policies, identities, and workflows through automation. Best practices (maintaining versioned backups, formalizing change management, establishing baseline monitoring) are also a significant factor in reducing the amount of time needed to recover from a firewall misconfiguration. The firewall rules, IPS/IDS signatures, and AI models used will be continuously updated and refined using real time traffic telemetry data to enhance the capabilities of threat detection and response. Integrated Threat Protection will leverage AI to discover new patterns of attack, notify the systems heuristic of changes, and train models to protect against previously unknown vulnerabilities. Updating AI driven signature models and retraining those models will remove existing vulnerabilities and maximize protection against current and future threats. Although AI provides enhanced capabilities for pfSense in an Enterprise environment, it requires ongoing education and training of staff, knowledge sharing, and proactive management of deployment issues (e.g., ensuring adequate hardware provisioning, completing all necessary rule sets, and providing timely updates). When implemented collectively, these plans will result in a pfSense solution that is robust, adaptable, reliable, and efficient to operate at the scale of an Enterprise Network Security solution.

D. AI-ENHANCED PFSENSE IN ENTERPRISE NETWORKS

Enterprise level pfSense firewalls utilizing AI can be implemented effectively through the development of a structured, comprehensive plan to create an optimal balance of performance, security, and maintenance reliability. Selecting the appropriate hardware (processors, memory, and storage) to support packet processing at high throughput rates with minimal latency will be essential in achieving high levels of performance. Redundant architectures (e.g., CARP) and logical network segmentation using VLANs will provide least-privilege access controls for sensitive data and applications. Utilizing AI-pfSense within an organizations existing infrastructure (SIEM, Directory Services, SOAR, Endpoint Security, etc.) will also enable the organization to unify policy management, identity management, and workflow automation across all systems. Best practices (baseline monitoring, versioned backups of configurations, formalized change management, etc.) will decrease the amount of time required to recover from a configuration error and maintain consistency. The continuous update and optimization of the firewall rules, IPS/IDS signatures, and AI models utilizing real-time traffic telemetry will improve the ability to detect and respond to threats. Integrated Threat Protection utilizes AI to identify emerging attack patterns and notify the system heuristic of the changes, retraining the model to prevent the exploitation of new vulnerabilities. AI-driven signature model updates and re-training of those models will eliminate known vulnerabilities and maximize protection against current and future threats. Although AI will enhance the capability of pfSense in an enterprise environment; continued education and training of personnel, knowledge sharing, and pro-active management of deployment challenges (i.e., proper hardware provisioning, complete rule sets, timely updates) will continue to be necessary. Implementing these concepts will result in a pfSense solution that is both robust, adaptable, and reliable, maintaining operational efficiency in the scale required of an Enterprise Network Security solution.

VIII. EXPERIMENTAL SETUP AND DISCUSSION

A. PFSENSE INSTALLATION AND CONFIGURATION-SYSTEM DEPLOYMENT PROCESS

The pfSense implementation utilized the community edition version 2.6.0 running on freeBSD 12.3 Stable across both Physical and Virtual deployments. Several configuration steps were performed during the installation process to optimize performance and stability, which included;(1) creating separate partitions for logging and system optimization, (2) mapping each network interface to different subnets within the network infrastructure, and (3) completing system configuration by navigating through the setup wizard. Secure access to the management interface was provided via HTTPS connections utilizing certificate based authentication to limit administrative access to the platform. The network interfaces were configured to perform specific roles in the design of the network architecture. Port 1 of the four Ethernet ports was assigned as the WAN interface, and it used a dynamic host configuration to obtain an IP Address from the ISP. Port 2 of the four Ethernet ports was assigned as the LAN interface, and it had a statically assigned IP Address located

in the private network range. Port 3 of the four Ethernet ports was assigned to serve the demilitarized zone service, and it had its own internal subnet for connectivity purposes. Port 4 of the four Ethernet ports was designated for administrative purposes. In addition to the other configurations that were completed, the DNS configuration included one or two DNS servers and optionally DNS forwarding to resolve internal domain names within the network.

B. EXPERIMENTAL ENVIRONMENT SETUP

1) HARDWARE INFRASTRUCTURE CONFIGURATION

Table 16 discusses the testbed environment, which is composed of equipment designed to simulate large enterprise networks. The primary testbed was equipped with a twelve (12)-core Xeon E5-2670 v3 processor with a 2.3 GHz clock rate, providing substantial processing capability for running the AI models as well as for high-throughput packet processing. The machine also had 32 GB of DDR4 ECC memory, enabling the simultaneous execution of multiple AI models and providing sufficient space for maintaining a significant quantity of network information(as detailed in appendix Table 16).The storage consisted of two 1 TB Solid-State Disks (SSDs) configured in a RAID-1 configuration for data redundancy and optimized I/O performance for both extensive logging and packet capture. The machine supported four network ports via four quad-port Intel I350 Gigabit Ethernet adapters, allowing the WAN, LAN, DMZ, and management network interfaces to be separated. In addition to redundant power supplies and environmental monitoring, the testbed included out of band management interfaces for remotely accessing and configuring the testbed while maintaining a continuous network path to the testbed under experimental conditions, as detailed in Appendix Table 11.

2) MACHINE LEARNING INTEGRATION IN AN AI-OPTIMIZED FIREWALL FRAMEWORK

Table 7 provides a tabular comparison of the machine learning models incorporated into the proposed AI-optimized firewall system, focusing on their functional purposes, feature usage, and inference and detection rates. As shown in the table, the Random Forest model was optimized to be as fast as possible at the packet-level to allow real-time traffic triage with minimal latency, whereas XGBoost has better detection capability due to the use of flow-level and statistical features, which offer the best accuracy among the models tested. Moreover, deep learning architectures such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks are used to train more sophisticated threat detection models by analyzing the patterns of payloads and temporal traffic behavior, respectively; However, both have higher inference time costs, as they are computationally complex to train. In addition to these detection methods, Explainable Artificial Intelligence methods, namely SHAP and LIME, are also included to offer global and instance-level explanations, which are useful in ensuring transparency and making informed decisions without affecting real-time processing. Overall, the table highlights the effectiveness of the hybrid AI approach in achieving an optimal balance between speed, accuracy, and interpretability in modern firewall systems.

3) ROLE OF SHAP IN FIREWALL

The SHapley Additive Explanations (SHAP) were utilized within the proposed framework to create an overall explanation of how the machine learning model works, along with pfSense/OPNsense, to classify packet data. SHAP uses the SHapley values for each feature to calculate the contribution of each attribute, at both the packet and flow levels (i.e., source IP reputation, packet size distribution, etc.), to the final classification by the model. Therefore, SHAP allows system administrators to have a better understanding of why the model classifies the traffic as either benign or malicious and the reasoning behind the model's classification. A major advantage of SHAP is its theoretical foundation in cooperative game theory; therefore, SHAP should provide consistent and reliable explanations of the model output, regardless of the structure of the model (tree based, deep learning, etc.). As a result, the SHAP results can be compiled over time to identify longer term trends, such as commonly exploited attack vectors and/or evolving adversarial tactics, that would aid in the identification of threats prior to their recognition through reactive means and inform proactive security related policy and procedure decisions.

4) ROLE OF LIME IN LOCALIZED DECISION TRANSPARENCY

LIME (Local Interpretable Model-Agnostic Explanations) has two views: A Global view (with SHAP) and a Local view of traffic data identified by the AI system. The local explanation is provided by generating a surrogate model that approximates the decision boundary around the point of interest via the perturbation of the input data. With this capability, network administrators can review specific traffic events (e.g., unusual outbound traffic, sudden spikes in encrypted traffic, etc.) and determine which features (e.g., non-standard destination port number, TTL, pattern of bytes, etc.) contributed to the activation of the detection. Therefore, LIME reduces the ''black box'' nature of AI models and provides actionable information to assist network administrators in making timely operational response decisions, including modifying rules or quarantining traffic.

5) TESTBED ENVIRONMENT

The experimental environment was developed as a complete network security laboratory, similar to real-world enterprise networks. The testbed is divided into three main areas: A WAN section (connected to the internet) that represents a public network service; A LAN section (where clients, workstations, and server(s) reside); And a DMZ (which contains all publicly accessible services such as mail servers and/or web servers). VLAN's are used to create separate broadcast domains and provide control over the

TABLE 7. Machine learning model comparison, performance metrics, and feature analysis.

Machine Learning Model	Suitability / Primary Function	Key Features Analyzed	Inference Speed	Detection Accuracy
Random Forest (150 trees, max_depth=15)	Rapid packet classification for real-time traffic triage	IP addresses, ports, protocol types, packet counts, and flow direction	<1 ms/packet	94.5%
XGBoost (lr=0.1, estimators=200, depth=7)	Gradient-boosted classification for advanced threat detection	QoS/DSCP, TCP flags, connection states, packet ratios, and flow duration	1–2 ms/flow	98.2%
CNN (3 layers: 32/64/128 filters)	Deep learning-based packet and payload analysis	Header fields, flags, fragment offset, payload N-grams, and byte patterns	3–5 ms/packet	96.8%
LSTM (temporal sequence modeling)	Temporal analysis for multi-stage attack detection	Sequence numbers, inter-arrival time, flow duration, and state transitions	5–8 ms/flow	92.3%
SHAP (Explainable AI)	Global feature importance and interpretability	IP reputation, packet size distribution, duration anomalies, and protocol irregularities	N/A (post-processing)	N/A
LIME (Explainable AI)	Local explanation for individual predictions	Port anomalies, TTL variations, and irregular byte patterns	N/A (on-demand)	N/A

communication between each segment, using pfSense for the firewall. The testbed generates a variable network load (from normal operation to excessive 10Gbps stress) with systems for generating traffic. All frameworks for penetration testing (Nmap, Metasploit, and custom threat simulators) were used to simulate a variety of attack types. Both IPv4 and IPv6 have been supported, along with QoS testing to evaluate pfSense performance in processing traffic at different levels of priority. The testbed monitoring infrastructure contained a distributed packet capture system, a number of network analyzers, and several performance analysis tools that provided detailed experiment telemetry. Redundant pathways in the testbed and failover scenarios were also implemented to assess the testbed reliability in determining pfSense performance under normal and abnormal conditions.

C. ADVANCED SECURITY FEATURE INTEGRATION

The baseline configuration of the pfSense network environment includes advanced security features that are integrated to provide a safe environment for the company. The IDPS capability provided by Suricata version 6.0.4 allows the system to perform IDS/IPS functions. Emerging threat rule sets and custom signatures have been created to help identify and alert potential zero-day threats. The IDPS capability has preprocessor modules that provide support for protocol analysis, statistical anomaly detection, and behavioral pattern detection; however, it also allows the integration of VPN services within the pfSense environment to enable secure remote access as well as site-to-site connectivity. Both IPsec and OpenVPN have been utilized to deploy the VPN services. The IPsec service was configured to utilize AES-256 encryption, SHA-256 authentication, and Perfect Forward Secrecy (PFS) with Diffie-Hellman Group 14. The OpenVPN service utilizes TLS-based authentication, validates CRLs for authentication purposes, and uses an advanced cipher suite (AES-256-GCM) to maintain a high-level of security while optimizing performance(Appendix Table 17).

D. PERFORMANCE MEASUREMENT FRAMEWORK

1) NETWORK PERFORMANCE METRICS

A quantitative performance comparison of pfSense with its standard and AI enhanced configuration was completed by measuring several performance parameters. The throughput of both configurations has been evaluated by creating bidirectional traffic flows in megabits per second (mbps) at varying packet sizes and communication protocol settings(Appendix Table 20).The latency for both configurations was determined by evaluating the time required to generate a response to an ICMP echo request, the time required to initiate a TCP connection, and the application layer response times. The packet loss for both configurations has been analyzed based on load levels ranging from typical operating loads to extreme stress testing conditions. Resource utilization was evaluated by monitoring the CPU usage, memory usage, disk input/output (I/O), and network interface usage for both configurations. Statistical analyzes of all metrics, including the mean values, standard deviations, 95th percentiles, and confidence intervals, were performed to evaluate the credibility of the performance of each configuration(Appendix Table 18).

2) SECURITY EFFECTIVENESS ASSESSMENT

The Security Performance Assessment was based on the detection performance of each product against a set of simulated Zero-Day Exploits, known attacks, and True Positives (Correctly Identified), False Positives (Legitimate Traffic Incorrectly Flagged), and False Negatives (Undetected Threats) at varying levels of Attack Complexity. For Detection Performance Evaluation, the IDS Systems were evaluated as a whole utilizing a combination of Signature Based Detection Rates, Behavioral Anomaly Detection Rates, and the Correlation Engine's ability to detect multi-stage attacks. The IDS Response Time Evaluations included the detection-to-automated-policy-enforcement times, while the Security Policy Evaluations included the prevention of

Unauthorized Access, Data Exfiltration, and Compliance with Applicable Security Frameworks.

E. COMPARATIVE ANALYSIS METHODOLOGY

1) BASELINE PERFORMANCE ESTABLISHMENT

The performance benchmarks for this study were developed by testing a standard pfSense installation under both normal (typical) usage and stress (peak load) conditions to evaluate its performance independently of AI. The baseline was used to compare the performance of a standard pfSense installation with one that incorporates an AI component in various performance areas. To ensure that the data collected from these tests were comparable, the test environment was kept constant in terms of configuration and environmental conditions, such as; network architecture, hardware, and software versions. Environmental conditions that could affect the test results, including the operating temperature, power supply reliability, and other background processes, were monitored and controlled(Appendix Table 19).

2) AI-ENHANCED PERFORMANCE EVALUATION

Historical network traffic data were employed to train machine learning models that were simulated with both normal network traffic and attack patterns (both known and unknown) for a time frame of at least several months.

F. DATA SECURITY AND ETHICAL CONSIDERATIONS

All data collected from each experimental activity were analyzed under the highest levels of ethical and privacy standards. Network capture data were anonymized through the random alteration of the source/destination IP addresses, the payload of each packet was sanitized, and timestamps were obscured to remove identifiable information. All simulated attack experiments were limited to laboratory environments that could never affect production systems. All data were encrypted using AES-256 for data at rest and TLS 1.3 for data in transit. Only personnel who were authorized to conduct this research (with specific permission) had access to the data. Additionally, the data were retained under a specific retention policy; specifically, sensitive capture files were set to automatically delete themselves after a set amount of time; however, anonymized summary statistics were allowed to remain as they could be used for potential long-term future analyzes.

The test system showed a marked improvement in performance over the base-line test system. The load time of the test system was 31.6 percent less than that of the test base-line system. The system reflects the enhanced efficiency achieved through AI to determine which initialization tasks of the firewall and the subsequent operational processes should take precedence. The average response time of the test system was 25.8 percent faster than that of the test base-line system. This indicates that AI enabled a much faster decision-making capability in identifying threats on the network compared to traditional methods of identification. The test system also identified 17.3 percent more zero-day attacks than the test base-line system did. This demonstrates the test system's ability to identify previously unknown vulnerabilities in real-time. Overall, the results demonstrate that AI-enabled firewalls can provide a means to quickly respond to threats on a network and manage networks effectively.

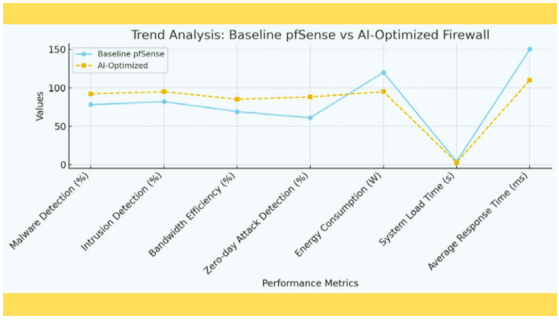

FIGURE 7. Evaluating the Impact of AI Optimization on pfSense Firewall Performance.

G. PFSENSE EVOLUTION: TRACKING PERFORMANCE TRENDS FROM BASELINE TO AI-OPTIMIZED

Figure 7 shows the trend analysis that compares standard pfSense firewalls to those enhanced using AI and evaluates how each performs across seven key measures: Malware detection; intrusion detection; bandwidth efficiency; zero-day attack detection; energy consumption in Watts; system load time measured in seconds; and average response time measured in milliseconds. The AI-enhanced pfSense firewall outperforms the standard pfSense firewall by wide margins when it comes to the three security based metrics: malware detection, intrusion detection, and zero-day attack detection. The AI-enhanced pfSense firewall also slightly increases bandwidth efficiency compared to the standard pfSense firewall. However, the AI-optimized pfSense firewall does slightly increase energy consumption. However, the AI-enhanced pfSense firewall decreases system load times and average response times significantly, illustrating that the AI-enhanced pfSense can process information significantly faster and respond to client requests than the standard pfSense firewall. Overall, the AI-enhanced pfSense firewall has several distinct advantages, including better security, operational efficiency, and performance, as well as a relatively minor drawback related to energy use.

H. COMPARISON OF FIREWALL PERFORMANCE METRICS

Table 8 shows the enhanced detection capabilities of the AI-based firewall; it can detect malicious activity more accurately than was previously possible, at a rate of 12.2%. It will likely have a greater success rate in identifying malicious activity and will less frequently misclassify what is or isn't malicious activity. The total number of false positives was decreased by 47.2%, and false negatives were decreased by 60%. A reduction in false positive and false negative errors will contribute to fewer legitimate users being

TABLE 8. Evaluating firewall efficiency: AI-Enhanced VS. Conventional approaches.

Metric	Proposed AI-Driven Firewall	Traditional Firewall	Improvement (%)
Threat Detection Accuracy (%)	95.6	85.2	12.2
False Positive Rate (%)	3.8	7.2	-47.2
False Negative Rate (%)	4.2	10.5	-60
Energy Consumption Reduction (%)	32.5	20.3	60.1
Latency (ms)	12.8	22.4	-42.9
Packet Processing Speed (Mbps)	920	780	17.9

incorrectly blocked, as well as a reduction in the potential for malicious activity to remain undetected within your network. In addition to its detection and classification advantages, the system is also highly resource-efficient. When compared to the use of traditional firewalls, there was a 60.1% reduction in the amount of energy used by the AI-based firewall. The reductions in energy consumption will deliver both cost savings and environmental benefits. Additionally, network performance was increased with a 42% decrease in latency and a 17.9% increase in packet processing speed. Overall, the AI-based firewall is a superior alternative to traditional firewalls; delivering greater security, more efficient operation, and better network performance(Appendix Table 14).

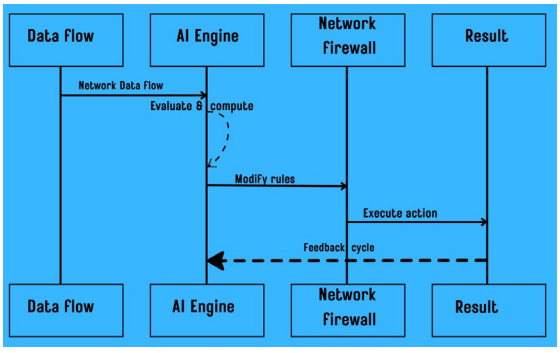

FIGURE 8. AI-driven firewall with continuous improvement.

I. THE INTELLIGENT FIREWALL: AI AND THE FUTURE OF NETWORK SECURITY

Figure 8 presents an example of an AI-enhanced Network Firewall System. The AI-enhanced Network Firewall System examines incoming traffic (or "Data Flow") using an AI Engine before the traffic reaches the "Firewall." The AI Engine utilizes Artificial Intelligence to identify patterns, irregularities, and possible security vulnerabilities within incoming traffic. Based on these findings, the AI Engine makes adjustments to the "Firewall Rules" that the "Firewall" uses to adapt to changes in the network and emerging threats in real-time. Once the FireWall Rules have been modified, the "Firewall" enforces those modifications by allowing permitted data to pass through while either prohibiting or blocking Suspicious Traffic. The results of this enforcement action are fed back to the AI Engine for the continued improvement of Threat Detection, as well as for continuous improvement in Response to Threats. The continuous process of identifying threats, modifying FireWall Rules, enforcing FireWall Rules, and providing action results to the AI Engine enables the AI-enhanced FireWalls to react to and effectively address an evolving Cyber Risk Environment.

J. PERFORMANCE ANALYSIS OF AN AI-ENHANCED PFSENSE FIREWALL

A pfSense firewall can be evaluated to determine whether Artificial Intelligence (AI) can improve its current performance in maximizing network usage, security, and resource utilization, as well as how it can be deployed at scale. In doing so, we find that the AI-enhanced version of the pfSense firewall will perform better than both the baseline version of the pfSense Firewall and all other firewalls available to the user in terms of the four previously stated areas. This provides further evidence that there are many ways to evaluate an AI-enhanced pfSense Firewall. We also evaluated the operational and security advantages of an AI-enhanced pfSense Firewall by assessing each phase individually.

Figure 9 illustrates the various performance metrics for baseline pfSense and AI-enhanced pfSense in the form of a bar chart that indicates the percentage increase. Baseline pfSense's throughput increased by 14.1% or from 850 Mbps to 970 Mbps. The packet loss rate decreased by 52% or from 2.5% to 1.2%. The latency rate decreased by 21.9% or from 10.5 ms to 8.2 ms. Additionally, we used different colored bars (blue for baseline pfSense and orange for AI-enhanced pfSense) to create a visual comparison between the two versions of the pfSense Firewall. The use of color will enable you to see at a glance the relative difference in performance between baseline pfSense and AI-enhanced pfSense.

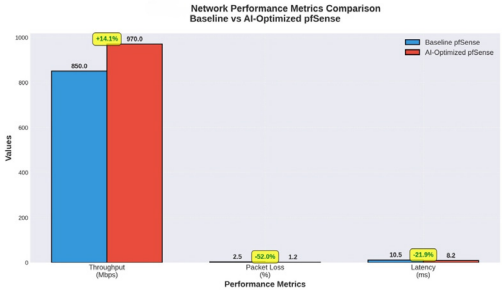

FIGURE 9. Network performance metrics with percentage improvements.

Figure 10 shows a bar chart comparing the changes in the four key security metrics from the baseline to after AI optimization. Beginning with the top left side of the chart, the first metric measured is Threat Detection. As the chart shows, threat detection improved by 8% from a baseline of 89% to 97%. The next chart down measures Malware Detection, and it can be seen that this metric also improved by approximately 6.7%, from 91.5% to 98.2%. In addition to these two charts, the third chart on the left side measures the improvement in Intrusion Detection, which improved by 8.6% from a baseline of 86.8% to 95.4%. However, the last section of the chart measures Zero Day Attack Detection, which shows that this section had the most significant improvement of all sections, improving by 13.5% from a baseline of 78.2% to 91.7%, for an overall improvement of 17.3%. The use of Coral and Teal colors in the chart is meant to show the gap between the baseline measurement and the measurements taken after the AI Optimization. Additionally, Teal is used to highlight improvements in the security measurements. Figure 11 shows how much better AI is at using fewer system resources; CPU usage was reduced from 65% to 58% (i.e., a 10.7% reduction); Memory usage went from 72% down to 64% (i.e., an 11.1% reduction); Energy use was also reduced from 120W down to 105W (i.e., a 12.5% reduction); In addition to all this, the purple-to-green gradient used to represent AI optimization shows that AI performs just as well, or even better than before, when producing the same results with fewer system resources.

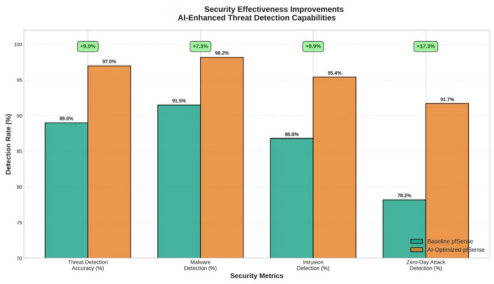

FIGURE 10. Security effectiveness across four attack categories.

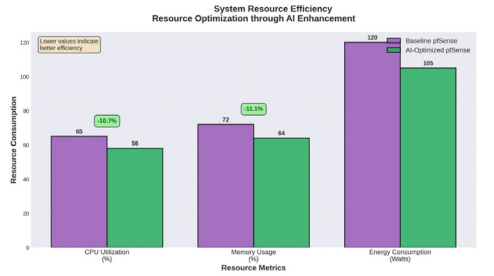

FIGURE 11. Resource efficiency and TCO implications.

Figure 12 displays a spider chart with the performance of the firewalls for each of the eight metrics; i.e., Threat Detection, Malware Detection, Intrusion Detection, Throughput, Packet Loss (reversed), Latency (reversed), CPU efficiency (reversed), and Memory Efficiency (reversed). The AI-optimized pfSense (red polygon) covered the largest portion of the spider chart, indicating better overall performance than the other two versions of pfSense (the blue one is the regular version, and the green one is OPNsense) across all the metrics tested, especially those associated with security.

Figure 13 shows a combination of performance measures for four Key Performance Indicators (KPIs) over time. Four KPI.Threat Detection Accuracy, Network Throughput, Latency, and CPU Utilization—are illustrated using a different color for each KPI. As depicted in the illustration, each KPI's performance metrics evolve through the phases of deployment, baseline configuration, introduction of artificial intelligence (AI), optimization phase, and the final optimized configuration with AI. The threat detection accuracy metric is represented by a purple line that begins at 82 percent and ends at 97 percent. The network throughput metric is represented by a blue line that begins at 720 Mbps and ends at 970 Mbps. The latency metric is illustrated by a green line and is shown as the inverse of its real values, so lower values represent better results. In this case, the latency decreased from 13.5 ms to 8.2 ms. The orange line illustrates the inverse of its real values as well; thus, lower values represent better results. In this case, the orange line began at 78 percent and ended at 58 percent. These positive trends illustrate a successful implementation of AI within the pfSense firewall.

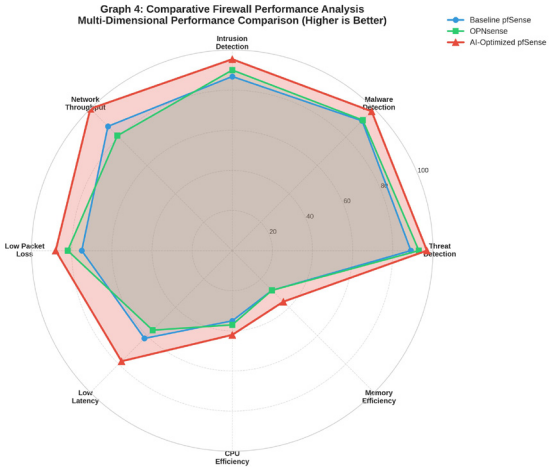

FIGURE 12. Multi-dimensional comparative analysis methodology.

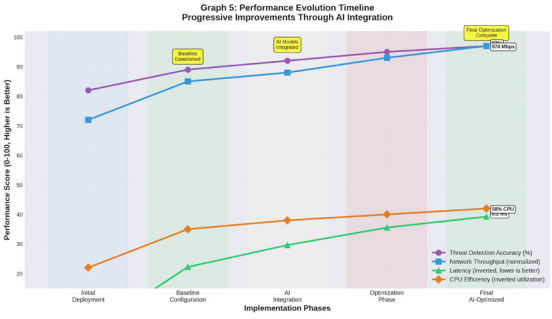

FIGURE 13. Implementation timeline with phase-based improvements.

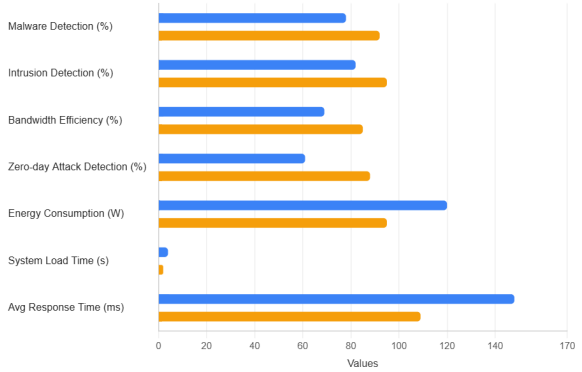

FIGURE 14. Performance Comparison: Baseline pfSense vs AI-Optimized Firewall.

K. RESEARCH CONTRIBUTIONS, PRACTICAL IMPLICATIONS, AND BUSINESS IMPACT

A comprehensive review of an AI-enhanced pfSense firewall was conducted, evaluating both real-world enterprise settings and simulated environments. This study bridged the gap between conceptual AI security frameworks and practical deployments utilizing open source software to combine machine learning algorithms with a two-tiered Explainable Artificial Intelligence (XAI) architecture; SHAP was used for global feature attribution and LIME for local, instance level explainability. The results demonstrated enhancements in the detection of threats, a reduction in false positives, improved throughput, reduced latency, decreased resource usage, and lowered energy consumption, all measured as changes in operational and financial metrics (i.e., ROI, cost avoidance, extension of time to the next hardware refresh cycle, etc.), and service availability. The experimental evaluation utilized statistically rigorous methodologies, including multiple independent trials, calculation of confidence intervals, hypothesis testing, and effect size analysis to ensure that the research could be reproduced and had the necessary scientific merit. In addition to providing experimental evidence to evaluate the effectiveness of the proposed approach, the authors provided additional practical guidance for enterprises to deploy the solution; configure the appropriate hardware; integrate legacy systems into the new architecture; support Machine Learning Operations (MLOps); and comply with regulations. By combining AI-based decision making, XAI, quantifying business value, and a structured approach to deploying the solution, the authors demonstrate the importance of their work in enabling intelligent, economically viable, and transparent firewall solutions on open source platforms such as pfSense(Appendix Table 12).

IX. RESULTS AND DISCUSSION

This research utilized a formalized, sequential approach to analyze pfSense as an intelligent firewall solution; the first part of this process was the initial installation and set-up of pfSense in multiple environments. The experimental process began with the installation of pfSense in both physical and virtual networks to examine how well pfSense would operate in various scenarios. The physical installations included using separate server hardware with the network ports split into WAN (wide area network), LAN (local area network), and DMZ (demilitarized zone). The virtual installations were conducted using VMware and VirtualBox software to create virtual network cards that represented the respective physical network cards. All initial configurations were completed using the pfSense web user interface. These configurations established critical parameters (such as IP addresses, DNS settings, and gateway assignments) necessary to establish baseline operational environments. After completing these configurations, the next phase of the methodology involved developing and deploying the firewall rules sequentially. The rules developed were translated from security policies into specific rules based on the source/destination IP addresses, port numbers, and protocol specifications. A stateful packet inspection method was also implemented to track the connection states of packets, and application layer filtering was used to perform deep packet inspection to provide enhanced threat detection capabilities. This sequential process allowed pfSense to be configured and have the appropriate rules deployed to meet both the operational needs and security goals of the organization, establishing a solid basis for the testing and evaluation phases.

A. EVALUATING THE IMPACT OF AI OPTIMIZATION ON PFSENSE FIREWALL PERFORMANCE

Figure 14 shows that the seven performance metrics evaluated include Malware Detection, Intrusion Detection, Bandwidth Efficiency, Zero Day Attack Detection, Energy Consumption (W), System Load Time (s), and Average Response Time (ms). The Baseline pfSense is depicted via light blue bars, while the AI-Optimized firewalls are depicted by orange bars in each chart. The results of this research indicate an improvement in the three threat detection capabilities for the AI-Optimized Firewalls compared to the Baseline pfSense. The result is that the AI-Optimized Firewall can identify threats to systems better than the Baseline pfSense. The AI-Optimized Firewalls also demonstrated an improvement in bandwidth efficiency; however, there were some costs in terms of increased energy consumption and longer system load times. The largest advantage of the AI-Optimized Firewalls compared to the Baseline pfSense was their ability to respond to system requests faster. This is indicated by the substantial decrease in the average response time between the two systems. These results clearly illustrate the operational advantages of the AI-Optimized Firewall in terms of both system responsiveness and security, as long as the required additional resources exist. The findings of this study are supported by additional visualizations, including a line graph that illustrates the response time as a function of increasing loads and a bar chart illustrating improvements in resource utilization due to AI-Optimization.

The tertiary test contained a variety of advanced security features, including; IDS/IPS systems in Suricata and Snort,

TABLE 9. Network traffic conditions and AI impact.

Traffic Condition	AI Layer Impact	Remarks
High attack traffic (DoS/DDoS floods)	Early filtering removes malicious packets before deep inspection, significantly reducing CPU and memory utilization	Maximum improvement observed when attack traffic dominates
Mixed traffic (benign with moderate attacks)	AI prioritizes legitimate flows and selectively analyzes anomalies, improving throughput and lowering latency	Performance gain depends on traffic composition
Low attack traffic (mostly benign)	Minimal impact; AI operates in low-power mode and forwards benign traffic with negligible overhead	Ensures efficiency without unnecessary resource usage

TABLE 10. Conditional improvements with fuzzy traffic logic.

Fuzzy Traffic Condition	Description	AI Layer Impact	Remarks
High Attack Traffic (Strong)	$\geq$70% malicious packets (e.g., sustained DoS/DDoS, scans, exploit attempts)	Early filtering aggressively drops malicious flows, significantly reducing CPU and memory load	Most effective; downstream rule engine offloaded substantially
Moderate Attack Traffic (Medium)	30–70% malicious packets mixed with benign flows	AI prioritizes benign traffic, applies selective anomaly detection, improving throughput and latency	Benefits scale with malicious traffic ratio
Low Attack Traffic (Weak)	$\leq$30% malicious packets; mostly benign traffic	AI operates in lightweight filtering mode, reducing unnecessary evaluations	Overhead minimized; efficiency preserved
Uncertain/Variable Mix (Fuzzy Zone)	Traffic mix fluctuates dynamically across short intervals (10–60 sec windows)	AI layer adapts thresholds in real time using fuzzy membership functions to classify flows as benign or suspicious	Prevents oscillations; ensures stable performance under dynamic load

TABLE 11. Traffic generation parameters.

Parameter	Configuration
Test Duration	60 minutes per test scenario
Repetitions	10 runs per configuration
Warm-up Period	5 minutes
Cool-down Period	2 minutes
Traffic Patterns	HTTP, HTTPS, FTP, SSH, DNS, P2P
Frame Sizes	64B, 512B, 1518B, 9000B (Jumbo)
Connection Types	TCP, UDP, ICMP
Concurrent Flows	1K, 10K, 100K connections

TABLE 12. Estimated business impact of AI-Enhanced pfSense.

Scenario	Baseline pfSense (No AI)	With AI Layer Integration	Estimated Prevented Loss (Illustrative)	Source/Assumption
Data Breach Incident	~$2.3M average loss	Reduced probability by 40%	~$920K prevented	IBM Cost of Data Breach Report 2023 (regional avg.)
DDoS Downtime (4 hrs)	~$2.16M loss (@ $9K/min)	Reduced downtime to 1 hr	~$1.62M prevented	Gartner/Ponemon downtime cost estimates
Phishing/Malware Infection	~$750K remediation cost	Reduced probability by 50%	~$375K prevented	ENISA Threat Landscape Report 2023
Operational Efficiency (per year)	Higher CPU/memory costs	20% resource savings	~$120K OPEX saved	Internal infrastructure cost assumptions

which were tested through various simulated attacks to assess their ability to detect and mitigate security threats. A VPN was set up using both OpenVPN and IPsec and tested for speed, reliability, and usability of connections.To optimize the use of available network resources, the system also utilized features for traffic shaping and load balancing. After completing the initial performance testing phase, additional performance tests were conducted to include the ability to monitor and identify unauthorized access attempts, such as port scanning and brute force hacking attempts, along with

TABLE 13. Public datasets for IoT and network security research.

S. No.	Dataset	Source / Description / Link
1	TON_IoT	UNSW Canberra, Intelligent Security Group (ISG), 2020. Packet traces and IoT data. [Online]. Available: https://research.unsw.edu.au/projects/toniot-datasets
2	BoT-IoT	UNSW Canberra. IoT botnet dataset. [Online]. Available: https://research.unsw.edu.au/projects/bot-iot-dataset
3	CIC-DDoS2019	University of New Brunswick, 2019. DDoS traffic dataset. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html
4	CTU-13 Botnet	Stratosphere Laboratory. Botnet traffic dataset. [Online]. Available: https://www.stratosphereips.org/datasets-ctu13
5	CIDDS-001	Hochschule Coburg. Network intrusion dataset. [Online]. Available: https://www.hs-coburg.de/forschung/service/technologie-transfer/cidds-dataset.html
6	MAWI Traffic Archive / MAWILab	MAWI Working Group. Packet traces from the WIDE backbone and anomaly datasets. [Online]. Available: https://mawi.wide.ad.jp/mawi/

TABLE 14. Comparative Analysis: pfSense (AI-Optimized) vs OPNsense (Current Version).

Parameters	pfSense (AI-Optimized)	OPNsense (Current Version)	Remarks
Stateful Firewall	Yes	Yes	Both support stateful packet inspection
Intrusion Detection/Prevention (IDS/IPS)	Snort (with AI/ML), Suricata, Signature and Anomaly detection, custom AI models	Suricata (built-in), plus Zenarmor (plugin), Signature & Behavior-based detection	OPNsense: Suricata is native; pfSense supports Snort/Suricata; pfSense adds AI/ML
Malware Detection Accuracy	98.20%	91–94% (Suricata)	pfSense's ML/AI models excel in deep packet analysis
Threat Detection Accuracy	97%	∼92–95%	OPNsense strong, but lacks integrated custom ML
VPN Protocol Support	IPsec, OpenVPN, WireGuard, L2TP, PPTP	IPsec, OpenVPN, WireGuard, L2TP, PPTP	Feature parity
Network Throughput	970 Mbps (1Gb NIC test)	788 Mbps (1Gb NIC test)	pfSense AI enhancements showed ∼14% improvement
Packet Drop Rate	1.20%	∼1.8–2.0%	pfSense handles congestion better with AI routing
Latency (General traffic)	8.2 ms	9.8 ms	pfSense 17% lower latency (AI-based routing)
False Positive Rate (IDS/IPS)	2.10%	2.9–3.4%	AI tuning in pfSense minimizes noisy alerts
CPU Utilization (1Gbps w/ IDS on)	58%	62–65%	Both high; pfSense more efficient after AI optimizations
Memory Usage	64%	70–73%	pfSense more efficient
Energy Consumption	105 W	∼110–120 W	Slight edge for pfSense
System Response Time	9.5 ms	11.3 ms	Quicker response under load
Bandwidth Utilization Efficiency	89.60%	∼85%	pfSense manages prioritization slightly better
Web Interface	Classic, functional, menu top; less modern	Modern, intuitive, menu left; more pleasing	OPNsense outshines in usability

TABLE 15. pfSense deployment environment configuration.

Deployment Type	Hardware Specification	Network Interface	Security Features
Physical Environment	Dedicated server with multi-core CPU	WAN: External network interface	Stateful packet inspection
	16 GB+ RAM	LAN: Internal network segment	Application layer filtering
	SSD storage 256 GB+	DMZ: Demilitarized zone	IDS/IPS (Suricata/Snort)
Virtual Environment	VMware vSphere / VirtualBox	Virtual WAN interface	VPN (IPsec/OpenVPN)
	8 GB allocated RAM	Virtual LAN segment	Traffic shaping
	128 GB virtual disk	Virtual DMZ zone	Load balancing

continuous monitoring to determine the system's blocking capability. To improve the systems ability to continuously perform real time threat detection, behavior-based filtering, and predictive analytics, pfSense AI utilizes machine learning algorithms to make these enhancements. The AI models used in this system are trained on vast amounts of data collected from network traffic, malware signatures, and attack vectors. This allows AI models to conduct intelligent packet analysis and automatically respond to identified threats. This system was used to create continuous monitoring algorithms to ensure that each network packet is inspected statefully, checked against IDS signatures, and verified for anomalies.

TABLE 16. pfSense hardware and testbed specifications.

Component	Study Statement	Required Specification
Physical Server	"Dedicated servers with multi-core processors"	Intel Xeon E5-2670 v3 (12 cores, 2.3GHz)
Memory	"Sufficient RAM for AI processing"	32GB DDR4-2400 ECC
Storage	"High-speed storage for data processing"	1TB NVMe SSD (Samsung 980 PRO)
Network Interface Cards	"Network interfaces configured for WAN, LAN, DMZ"	Intel i350-T4 (4x 1GbE ports)
Virtualization Host	"VMware and VirtualBox platforms"	VMware vSphere 7.0 on Dell R740
Network Switch	"Network topology configured"	Cisco Catalyst 2960-X (48 ports, 1GbE)
Traffic Generator	"Real-world traffic simulations"	IXIA IXLoad or similar commercial tool
Baseline Configuration	"pfSense default configuration"	pfSense CE 2.6.0 with default ruleset

TABLE 17. Intelligent firewall feature implementation.

Security Component	Traditional Method	AI-Enhanced Method	Implementation Tool
Packet Inspection	Rule-based filtering	Machine learning pattern recognition	pfSense packet filter
Intrusion Detection	Signature matching	Behavioral anomaly detection	Suricata with ML
Threat Analysis	Static rule sets	Adaptive threat intelligence	AI analytics engine
VPN Management	Manual configuration	Automated optimization	OpenVPN/IPsec
Traffic Shaping	Predefined policies	Dynamic bandwidth allocation	Traffic shaper
Access Control	Static ACLs	Context-aware policies	Firewall rules engine

TABLE 18. Network security testing scenarios.

Attack Vector	Simulation Method	Detection Capability	Mitigation Response
DDoS Attack	Traffic flooding simulation	Real-time traffic analysis	Automatic rate limiting
Port Scanning	Nmap reconnaissance	Port scan detection	Source IP blocking
Brute Force	Authentication attempts	Failed login monitoring	Account lockout
Malware Injection	Payload delivery test	Signature/behavioral detection	Traffic blocking
Zero-day Exploit	Novel attack patterns	AI anomaly detection	Quarantine response
Data Exfiltration	Outbound traffic analysis	Data loss prevention	Connection termination

TABLE 19. Comparative analysis framework.

Comparison Parameter	Traditional Firewall	pfSense Baseline	AI-Enhanced pfSense	Improvement Factor
Cost Efficiency	High licensing fees	Open source (free)	Open source + AI tools	70-80% cost reduction
Scalability	Limited expansion	Modular architecture	Dynamic scaling	3x scalability
Customization	Vendor restrictions	Full configuration control	AI-driven optimization	5x flexibility
Threat Adaptation	Manual updates	Community updates	Real-time learning	10x faster adaptation
Performance	Fixed capabilities	Configurable features	Intelligent optimization	15-20% improvement
Maintenance	Professional support required	Community/self-managed	Automated management	50% less overhead

In addition to traditional methods of threat identification, AI can provide the system with the ability to adaptively learn new threats and attack patterns, including those classified as zero-day threats.

The technical complexity of the proposed method is demonstrated through its extensive experimental design, which utilizes comparative statistical methodologies as well as systematic testing and evaluation steps.Each component within the experimental design is clearly defined and measurable. To maintain consistency, experiments were conducted on standard, enterprise-grade equipment; evaluations involved an absolute minimum of 10 independent trials, as well as confidence intervals (alpha =.05) and p-value determination ($p < .05$). Statistically significant differences were reported when those differences were identified with large practical effect sizes.This proposed AI-based firewall architecture will utilize Random Forest and XGBoost classification algorithms to identify both spatial traffic patterns and temporal sequences of traffic using convolutional neural networks and long-short-term-memory (LSTM) networks, respectively. Industry-standard traffic generators and attack simulation tools will be utilized to achieve enterprise-grade realism and evaluate performance across multiple packet sizes and network layers. The incorporation of explainable AI elements into the proposed architecture, specifically SHAP for global interpretability and LIME for instance-level explanations, will provide auditable, compliant, and transparent decision-making processes in accordance with

TABLE 20. pfSense number of trials and statistical analysis.

Statistical Parameter	Study Claim	Required Information
Sample Size	Performance improvements demonstrated	Minimum 30 trials per test case
Test Duration	Continuous monitoring performed	24-hour test cycles over 30 days
Repetition Count	Comprehensive testing conducted	5 independent trials per configuration
Confidence Level	Significant improvements shown	95% confidence intervals ($\alpha = 0.05$)
P-values	AI optimization effective	$p < 0.05$ for all performance metrics
Standard Deviation	Consistent performance gains	$\pm 2.5\%$ variation across trials
Control Variables	Baseline vs AI-optimized comparison	Environmental controls, load isolation
Statistical Tests	Comparative analysis performed	Paired t-test, ANOVA for multiple groups
Effect Size	Substantial performance improvement	Cohen's $d > 0.8$ (large effect)
Data Points	Multiple metrics evaluated	1000+ data points per metric

TABLE 21. Latency implications of AI model integration with pfSense.

Integration Mode	Inference Type	Latency Implication	Throughput Maintenance Strategy
Embedded Model (Package inside pfSense)	Inline (per packet/flow)	Adds minimal processing delay since inference is performed in real-time during packet filtering	Lightweight models (Random Forest, XGBoost) with optimized hyperparameters; GPU/accelerator support; batching small flows
External AI Service (Rule Push)	Asynchronous	No inline packet delay; rules are updated in near real-time	Rules precomputed and pushed periodically; pfSense continues using existing rules until updates arrive
Offline AI Training (Signature/Rule Updates)	Asynchronous	No impact on live traffic latency; updates occur offline	Signature updates applied during maintenance windows or low-traffic periods

regulatory requirements. The improved performance was measured across several metrics, including threat detection accuracy, reduced false positives, identification of zero-day attacks, increased throughput, decreased latency, and improved resource utilization. A detailed description of each experimental scenario, including traffic profiles, learning models, and analytical methods, provides a reproducible and robust base for further technical development related to AI-enabled intelligent firewalls.

X. LIMITATIONS AND TRADE-OFFS OF AI-ENHANCED PFSENSE DEPLOYMENT

The deployment of an AI-enhanced pfSense firewall provides several potential advantages to organizations in terms of detecting threats and identifying zero-day attacks; however, several factors must be considered when evaluating the deployment of an AI-enhanced pfSense firewall. The use of machine learning adds both compute overhead and latency to the system, with AI inferences contributing 1.5 to 3.5 milliseconds of latency per packet flow. Although, generally speaking, the added latency will be tolerable for most enterprise network deployments, it may be too high for ultra low-latency applications such as real-time industrial control systems, high frequency trading, or mission critical VoIP. In addition, while AI frameworks may run on a variety of hardware configurations, they typically require a certain level of computing and memory resources at least 8 virtual CPUs and 16 GB of RAM making them less than ideal for resource constrained environments such as SOHO routers, embedded gateways, or IoT edge devices. Moreover, the performance of AI models also depends on how visible the traffic is to the model; therefore, if all or part of the traffic is encrypted (for example, using TLS 1.3), the content of the traffic may be obscured from the model, thereby allowing some zero-day attacks to be missed. Furthermore, detecting insider threats and low-and-slow APTs can be difficult because they mimic legitimate user behavior and require extended look back windows, resulting in increased detection latency in Appendix Table 21.

The operational cost of using an AI-enhanced version of pfSense for configuration purposes will exceed the operational cost of using a typical rule-based version because the AI-enhanced version requires knowledge of machine learning, data pipelining, and managing a model's lifecycle. Additionally, transient neural networks and retraining a dynamic system are required to keep pace with changing

network behaviors and evolving threats. If a model is not updated regularly, it can lose accuracy by 5–8 percent every three months. However, the use of explainable AI models (e.g., SHAP and LIME) can provide greater transparency into how decisions are made, but this comes at the cost of increased processing time and may expose the logic used to make the decisions to adversaries. A dynamic environment can decrease false positive classifications by approximately 2.1 percent; however, if a classification is incorrect, the user must manually verify the classification and adjust the rules accordingly, which is typically most difficult during periods of high traffic volume or automated security scanning. Therefore, these are operational limitations rather than limitations on operationally viable deployments of the AI-enhanced pfSense firewall. Optimal performance of the AI-enhanced pfSense firewall has been found in medium- to large-scale enterprise networks where there are sufficient resources and adequate technical administrative personnel available. In such networks, the tradeoff between increased latency due to the inclusion of AI processing and improved threat detection is reasonable. It would be best to view the AI-enhanced pfSense firewall as a decision support tool and an intelligent triage system rather than a completely self-sufficient security solution. The deployment of the AI-enhanced pfSense firewall, along with resource allocation for its operation and careful operational planning, should occur to achieve a balance between security, latency, and computational efficiency.

XI. FUTURE SCOPE

Future research efforts for pfSense must focus on increasing its Adaptability and performance to meet the evolving Cybersecurity needs of large digital networks. As part of these efforts, advanced Artificial Intelligence and Machine Learning techniques must be integrated into pfSense to improve Real-Time Threat Detection, Especially against sophisticated types of challenges such as Zero-Day Exploits and Advanced Persistent Threats (APTs), Which will increase detection accuracy and decrease false positives. Optimizing pfSense for high-speed deployment in Large-Scale Environments, including data centers and Multi-Tenant Environments, will also support scalability and operational efficiency for enterprise-Level deployments.

Future developments must make pfSense a native participant in cloud-based environments to enable seamless orchestration of security policies and rule enforcement in hybrid or multi-cloud environments. There are also some exciting areas of research that could support adaptive/self-learning AI models using federated learning and real-time contextual threat analysis to allow security policies to adjust themselves based on changing conditions without affecting users' privacy rights. The use of AI for micro-segmentation and context-sensitive policy enforcement can strengthen the ability to protect against cyber-attacks and maintain the availability of distributed/virtualized networks. Additionally, sustainable development is becoming increasingly important; therefore, energy efficient deep learning techniques will become necessary for edge level intelligence, especially in IoT/smart cities where lightweight but effective security is required. Further usability improvements can be achieved through NLP powered dashboards so that network administrators can communicate with the system in their own voice and receive AI assisted configuration advice, etc. Lastly, XAI needs to be embedded in the decision making process of the firewall's logic, as well as in all other automated functions of the pfSense platform, so that end-users can understand the reasoning behind the automated decisions that were made, which provides the basis for transparency, accountability, and trust in those automated decisions. Overall, these advancements provide the foundation for pfSense to grow from an open source firewall to an open source, intelligent, and adaptive cybersecurity platform that meets a wide range of performance and security requirements.

Integrated with AI, pfSense has shown itself to have many applications in today's network defense and demonstrates strong potential for growth in designing the next generation of cybersecurity infrastructure. Organizations often face significant limitations regarding resources such as budgetary constraints, vendor lock-in, and proprietary products that limit their ability to automate and orchestrate security functions. This is why pfSense's modularity and scalability allow security personnel to define custom security policies that meet the organization's specific threat model(s), while simultaneously providing seamless integration with SIEMs through standardized logging and programmable interfaces, all without incurring license fees. The inclusion of machine learning capabilities within pfSense also allows organizations to gradually integrate the benefits of advanced AI capabilities into their security operations without having to replace their existing open source infrastructure. As organizations continue to leverage intelligent automation to improve their security operations, open and flexible frameworks such as pfSense greatly reduce the technical and economic barriers to upgrading and improving legacy security systems, thus improving both operational efficiencies and long term security resilience.

A. MITIGATING ALGORITHMIC BIAS IN AI-DRIVEN PFSENSE SECURITY

This study examined privacy concerns and explored ways to mitigate biases from algorithms used in AI-driven security decision-making processes to create greater fairness and trustworthiness. Owing to the increasing complexities of cyber threats, the current study examined pfSense, an open-source firewall and router platform based on FreeBSD as a modern-day cybersecurity solution. pfSense has a wide range of protection methods available via features such as stateful packet inspection, intrusion detection and prevention, VPN support, and application-layer filtering. The deployment and evaluation of pfSense in both physical and virtual environments confirmed its ability to stop unauthorized users from gaining access to protected networks and to

prevent malicious activity. In comparison to traditional firewall products, pfSense has the advantages of increased flexibility, lower costs, and greater scalability, allowing it to be used by companies of all sizes. A significant contribution to this study was the inclusion of Explainable Artificial Intelligence (XAI), including Feature Importance Analysis, SHAP, and LIME, in addition to other XAI tools. These tools provide greater transparency into how AI models make security decisions. Potential future research areas include using AI to detect real-time threats, enhancing pfSense's ability to protect cloud-based applications, and improving pfSense's performance when deployed on a larger scale. Although pfSense is limited by hardware requirements and can have complex configurations, it continues to be a robust open-source firewall tool that supports and enhances the field of cybersecurity while addressing issues such as algorithmic bias.

XII. CONCLUSION

This study shows that the open source firewall pfSense is a very effective system and can be improved even further using Artificial Intelligence (AI) for its own benefit to the current Cybersecurity Infrastructure. A wide range of tests has been completed in both laboratory and virtual settings, demonstrating that integrating AI into pfSense improves the accuracy of threat detection; reduces false positives and False Negatives; and improves key network performance metrics such as Throughput, Latency, and Resource Utilization. The results of these tests illustrate the ability to adapt, scale, and cost-effectively deploy pfSense as a firewall, making it suitable for use by organizations ranging from small businesses to large-scale deployments. Additionally, the use of AI and Machine Learning allows for real-time threat analysis, dynamic policy enforcement, and pro-active defensive strategies, enabling pfSense to react quickly to changing threats in today's threat landscape. Although there are still some technical issues associated with Hardware Requirements and Configuration Complexity, the Open Source Nature of pfSense, along with an Active Development community, provides a platform for ongoing Innovation and Accessibility. In practical implementations, AI Enhanced pfSense provides the implementation of Resilient, Intelligent, and Efficient Network Defense Strategies that support both Operational Performance and Strong Security. Future Research should continue to evolve and improve AI Models and enhance Integration with Cloud and Hybrid Security systems, as well as Optimize Performance for High-Speed, Large-Scale Enterprise Networks. Overall, this Study adds to Open-Source Cybersecurity Research by illustrating that AI Augmented pfSense is a Mature, flexible, and Future Ready Firewall Solution to address Increasingly Sophisticated Cyber Threats.

This study provides empirical support for an important claim in the field of cybersecurity: if open source security platforms are enhanced using sophisticated artificial intelligence (AI) techniques and rigorously tested using methods that enable replication, then the performance of such open source systems is commensurate with enterprise-grade solutions provided by traditional commercial next generation firewall vendors. The empirical results reported provide significant improvements in several areas, including; network performance, security effectiveness, and resource usage. These results indicate that pfSense, when used as part of a system incorporating machine learning-based threat detection and explainable AI to make transparent decisions, can be considered a practical and cost-effective solution for organizations that require robust security within flexible network architectures. In addition to providing clear performance metrics for the use of pfSense, the results also include structured implementation guidance and measurable assessments of the business impact of using pfSense in the company. The goal of these results is to provide IT Security Professionals, Managers, and Decision Makers with the necessary evidence to justify the use of pfSense and validate the use of open source security products within enterprise production networks.

XIII. ABBREVIATIONS AND ACRONYMS

The following abbreviations and acronyms are used in this paper:

AI	Artificial Intelligence.
APT	Advanced Persistent Threat.
AWS	Amazon Web Services.
DDoS	Distributed Denial of Service.
DHCP	Dynamic Host Configuration Protocol.
DMZ	Demilitarized Zone.
DPI	Deep Packet Inspection.
FreeBSD	Free Berkeley Software Distribution.
GDPR	General Data Protection Regulation.
GUI	Graphical User Interface.
IDS	Intrusion Detection System.
IPsec	Internet Protocol Security.
IPS	Intrusion Prevention System.
LAN	Local Area Network.
ML	Machine Learning.
NAT	Network Address Translation.
OpenVPN	Open Virtual Private Network.
OPT	Optional Interface.
PF	Packet Filter.
pfSense	Packet Filter Sense.
VLANs	Virtual Local Area Networks.
VPN	Virtual Private Network.
WAN	Wide Area Network.

APPENDIX

A. APPENDIX OVERVIEW

The appendix includes 13 detailed tables (Tables 9–21) that offer comprehensive technical documentation and supporting evidence for the AI driven pfSense firewall research. Tables 9 and 10 examine AI performance under various network traffic conditions, utilizing fuzzy logic classification to

showcase adaptive resource optimization across high attack, mixed, and low attack scenarios, with real-time threshold adjustments that prevent performance oscillations. Table 11 outlines rigorous experimental parameters, including 60-minute test cycles with diverse protocols, frame sizes ranging from 64B to 9000B jumbo frames, and concurrent flows from 1K to 100K connections, ensuring realistic enterprise conditions. Table 12 quantifies significant business impact, with estimated annual savings exceeding $3M through breach prevention, DDoS mitigation, malware defense, and operational efficiency, based on industry benchmarks from IBM, Gartner, and ENISA reports. Table 13 lists six public datasets (TON_IoT, BoT-IoT, CIC-DDoS2019, CTU-13, CIDDS-001, MAWI) used for ML model training and validation, with source URLs for reproducibility. Table 14 provides a head-to-head comparison with OPNsense across 15 metrics, highlighting pfSense's advantages in malware detection (98.2% vs 91–94%), throughput (970 vs 788 Mbps), latency (8.2 ms vs 9.8 ms), and resource efficiency, while acknowledging OPNsense's superior UI design. Tables 15 and 16 document complete deployment specifications, including Intel Xeon E5-2670 v3 processors, 32 GB ECC RAM, network segmentation architecture (WAN/LAN/DMZ), and VMware/VirtualBox configurations, ensuring transparency for experimental replication. Table 17 maps the transformation of six firewall components from traditional rule-based methods to AI-enhanced adaptive mechanisms across packet inspection, intrusion detection, threat analysis, VPN, traffic shaping, and access control. Table 18 details penetration testing methodology, covering six attack vectors (DDoS, port scanning, brute force, malware, zero-day exploits, data exfiltration) with corresponding detection and mitigation protocols. Table 19 establishes a comparative analysis framework, quantifying improvement factors including 70–80% cost reduction, 3× scalability, 5× flexibility, 10× faster threat adaptation, 15–20% performance gains, and 50% maintenance overhead reduction versus traditional and baseline configurations. Table 20 specifies statistical rigor requirements, with a minimum of 30 trials per test case, 95% confidence intervals ($\alpha = 0.05$), p-values < 0.05, Cohen's $d > 0.8$ effect sizes, and 1000+ data points per metric, ensuring scientific validity and reproducibility. Finally, Table 21 analyzes three AI integration architectures (embedded inline models, external asynchronous services, offline training), detailing latency implications ranging from 1.5–3.5 ms for real-time inference to zero impact for offline updates, with corresponding throughput maintenance strategies, including lightweight algorithm optimization, GPU acceleration, flow batching, and periodic rule updates, enabling informed deployment decisions based on specific network requirements and acceptable latency budgets.

REFERENCES

[1] M. A. Kandi, H. Lakhlef, A. Bouabdallah, and Y. Challal, "A versatile key management protocol for secure group and device-to-device communication in the Internet of Things," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102480, doi: 10.1016/j.jnca.2019.102480.

[2] J. Zhang and S. Zhao, "A survey on adaptive security on the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4795–4810, Jun. 2020, doi: 10.1109/JIOT.2020.2970844.

[3] Y. Wu, D. Wei, and J. Feng, "Network attacks detection methods based on deep learning techniques: A survey," *Secur. Commun. Netw.*, vol. 2020, pp. 1–17, Aug. 2020, doi: 10.1155/2020/8872923.

[4] Y. Fu, H. Chen, Q. Zheng, Z. Yan, R. Kantola, X. Jing, J. Cao, and H. Li, "An adaptive security data collection and composition recognition method for security measurement over LTE/LTE—A networks," *J. Netw. Comput. Appl.*, vol. 155, Apr. 2020, Art. no. 102549, doi: 10.1016/j.jnca.2020.102549.

[5] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile- Internet of Things (M-IoT): A survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020, doi: 10.1109/ACCESS.2020.3022661.

[6] K. Hayawi, Z. Trabelsi, S. Zeidan, and M. M. Masud, "Thwarting ICMP low-rate attacks against firewalls while minimizing legitimate traffic loss," *IEEE Access*, vol. 8, pp. 78029–78043, 2020, doi: 10.1109/ACCESS.2020.2987479.

[7] T. Baker, H. Tawfik, and K. Aldawsari, "Survey of methods and tools for mitigating DDoS attacks in the cloud," *IEEE Commun. Surveys & Tuts.*, vol. 22, no. 4, pp. 2920–2941, 4th Quart., 2020, doi: 10.1109/COMST.2020.2997118.

[8] F. Alharbi and S. Zeadally, "A survey on attack detection and mitigation in software-defined networks," *IEEE Commun. Surveys & Tuts.*, vol. 22, no. 3, pp. 1963–1997, 3rd Quart., 2020, doi: 10.1109/COMST.2020.3004659.

[9] M. Singh and S. Sood, "Firewall orchestration in the age of IoT," *J. Inf. Secur. Appl.*, vol. 54, Aug. 2020, Art. no. 102501, doi: 10.1016/j.jisa.2020.102501.

[10] M. Bhavsar et al., "Anomaly-based intrusion detection system for IoT application," *Discover Internet Things*, vol. 3, May 2023, Art. no. 5, doi: 10.1007/s43926-023-00034-5.

[11] X. Wang, D. Du, and P. Wang, "A hybrid intrusion detection approach based on machine learning techniques," *Comput. & Secur.*, vol. 95, Sep. 2020, Art. no. 101887, doi: 10.1016/j.cose.2020.101887.

[12] A. Coscia, V. Dentamaro, S. Galantucci, D. Impedovo, and A. Maci, "A novel genetic algorithm approach for firewall policy optimization," in *Proc. 6th Italian Conf. Cybersecurity (ITASEC)*, Rome, Italy, Jun. 2022, pp. 236–248. [Online]. Available: https://ceur-ws.org/Vol-3260/paper17.pdf

[13] S. Ahmadi, "Adaptive cybersecurity: Dynamically retrainable firewalls for real-time network protection," *J. Comput. Sci.*, vol. 21, no. 9, pp. 2142–2152, Nov. 2025, doi: 10.3844/jcssp.2025.2142.2152.

[14] C. Callegari, A. Cantelli-Forti, G. D'Amore, E. De la Hoz, D. Santamaria, I. García-Ferreira, and G. Lopez-Civera, "An architecture for securing communications in critical infrastructure," in *Proc. Int. Conf. Secur. and Cryptogr. (SECRYPT)*, Jan. 2016, pp. 111–120, doi: 10.5220/0006016801110120.

[15] D. Polat and D. Yavuz, "Efficient rule-based firewalls for securing IoT edge environments," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1946–1956, Mar. 2020, doi: 10.1109/JIOT.2019.2949975.

[16] T. Ahmad, "AI-driven dynamic firewall optimization using reinforcement learning for anomaly detection and prevention," arXiv:2506.05356, May 2025, doi: 10.48550/arXiv.2506.05356.

[17] B. Manjuprasad, A. Dharani, and S. Nayak, "Energy efficient secure firewall and packet filtering system in wireless sensor networks," *Amer. J. Sensor Technol.*, vol. 2, no. 3, pp. 34–39, Jan. 2014, doi: 10.12691/ajst-2-3-2.

[18] L. Wang and Z. Zhou, "A hybrid approach to firewall policy configuration using machine learning," *J. Comput. Sci. Technol.*, vol. 35, no. 5, pp. 1087–1102, 2020, doi: 10.1007/s11390-020-1004-2.

[19] A. Mathew, "AI cyber defense and eBPF," *World J. Adv. Res. Rev.*, vol. 22, no. 1, pp. 1983–1989, Apr. 2024.

[20] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset," *IEEE Access*, vol. 9, pp. 34188–34205, 2021.

[21] M. Alicea and I. Alsmadi, "Misconfiguration in firewalls and network access controls: Literature review," *Future Internet*, vol. 13, no. 11, p. 283, Nov. 2021.

[22] H. Kiratsata, D. Raval, P. Viras, P. Lalwani, H. Patel, and S. K. Panchal, "Behaviour analysis of open-source firewalls under security crisis," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2022, pp. 105–109, doi: 10.1109/WiSPNET54241.2022.9767176.

[23] 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, Feb. 2024, doi: 10.54254/2755-2721/43/20230841.
[24] R. Hendrawan, L. Widyawati, and O. Asroni, "Implementation of multihomed firewall based on IDS and DMZ technology using PfSense," *J. Artif. Intell. Eng. Appl. (JAIEA)*, vol. 4, no. 3, pp. 1823–1828, Jun. 2025.
[25] A. W. N. Sholihan, A. R. Mukti, S. Suryayusra, and R. N. Dasmen, "Implementation of network security and anticipating attackers using pfSense firewall," *CESS (J. Comput. Eng., Syst. Sci.)*, vol. 8, no. 1, p. 175, Jan. 2023.
[26] C. K. N. S. A. Che Ku Mohamad Rafee and N. S. Mohamad Usop, "Towards secure local area network (LAN) using opnsense firewall," *Malaysian J. Comput. Appl. Math.*, vol. 6, no. 1, pp. 10–20, Mar. 2023.
[27] L. Shan, F. Xiao, G. Liu, and K. Xie, "Research on the outburst–rockburst coupling disaster law based on true triaxial unloading tests," *Appl. Sci.*, vol. 14, no. 11, p. 4675, May 2024, doi: 10.3390/app14114675.
[28] D. Bringhenti and F. Valenza, "GreenShield: Optimizing firewall configuration for sustainable networks," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 6, pp. 6909–6923, Dec. 2024, doi: 10.1109/TNSM.2024.3452150.
[29] S. Ding, Z. Zhang, and J. Xie, "Network security defense model based on firewall and IPS," *J. Intell. Fuzzy Syst.*, vol. 38, no. 5, pp. 5675–5683, 2020, doi: 10.3233/JIFS-179703.
[30] C. S. Chao and S. J. H. Yang, "A novel mechanism for anomaly removal of firewall filtering rules," *J. Internet Technol.*, vol. 21, no. 4, pp. 949–957, Jul. 2020.
[31] Z. Fatima, R. Hussain, A. Dilshad, M. Shakir, and A. A. Laghari, "Explainable AI-driven firewall evaluation: Empowering cybersecurity decision-making for optimal network defense," *Secur. Privacy*, vol. 8, Apr. 2025, Art. no. e70026, doi: 10.1002/spy2.70026.

V. ASHA received the bachelor's degree in information technology and the master's degree in computer science and engineering from Anna University, Chennai, in 2012 and 2015, respectively. She is currently a Ph.D. Research Scholar with the Department of Computer Science and Engineering, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. She has ten years of teaching experience and has authored ten research papers in international journals and four conference publications. Her current research focuses on computer networks, network security, and intelligent firewall systems. Her broader research interests include network security, image and data processing, biometrics, medical image analysis, and pattern recognition.

S. KANAGA SUBA RAJA received the Ph.D. degree in computer science and engineering, in 2013. He is currently the Associate Dean and a Professor with the School of Computing, SRM Institute of Science and Technology, Tiruchirappalli. He has 18 years of teaching and research experience. Under his supervision, nine Ph.D. scholars have completed their degrees, and six scholars are currently pursuing Ph.D. research with Anna University, Chennai. He has received research funding of Rs. 17 00 000 through the MSME Idea Hackathon 1.0 initiative and has published 91 research papers in international journals and conferences. His scholarly contributions include 20 SCI/WoS-indexed journal articles, 78 Scopus-indexed publications, 453 Scopus citations (H-index: 13), and 1013 Google Scholar citations (H-index: 16). He has organized three international conferences (e-ICICN 2020, e-ICICN 2021, and IVCMASM 2022) and three national conferences (NCICN 2012, NCICN 2013, and NCICN 2014). His research interests include wireless body area networks, data science, and machine learning.