Analyzing the Impact of Smart Firewall Implementation on Cyberattack Protection

تحليل تأثير تنفيذ الجدار الناري الذكي على الحماية من الهجمات السيبرانية

فادي مازن جميل Fadi Mazin Jamel

جامعه الاداب و العلوم والتكنولوجيا في لبنان
(AUL) Arts, Sciences, and Technology University In Lebanon
fma072@live.aul.edu.lb

تاريخ تقديم البحث :2025/04/02
تاريخ قبول النشر :2025/40/09

Abstract

This research examines the impact of smart firewalls on cybersecurity, comparing them to traditional firewalls. It highlights several advantages of smart firewalls, including machine learning, deep packet analysis, and automated threat response. The study tests a smart firewall in a simulated network under various cyber-attack scenarios, measuring threat detection rates, response times, and network performance.

The results indicate that the smart firewall significantly outperformed traditional firewalls, achieving a malware detection rate of 93.94%, a phishing detection rate of 88.89%, and a DDoS detection rate of 96.77%. Additionally, it demonstrated faster response times and had minimal impact on network performance. However, it did exhibit a higher false alarm rate for phishing attempts.

In conclusion, the research suggests that smart firewalls improve protection against evolving cyber threats. It recommends investing in more accurate algorithms to reduce false alarms and integrating these systems with other security solutions to ensure comprehensive protection.

المستخلص

يحلل هذا البحث تأثير الجدران النارية الذكية على الأمن السيبراني، مع مقارنتها بالجدران النارية التقليدية. ويسلط الضوء على عدة مزايا للجدران النارية الذكية، بما في ذلك التعلم الآلي، وتحليل الحزم العميق، والاستجابة التلقائية للتهديدات. تم اختبار جدار ناري ذكي في شبكة محاكاة تحت سيناريوهات مختلفة للهجمات السيبرانية، حيث تم قياس معدلات اكتشاف التهديدات، وأزمنة الاستجابة، وأداء الشبكة.

أظهرت النتائج أن الجدار الناري الذكي تفوق بشكل كبير على الجدران النارية التقليدية، حيث حقق معدل اكتشاف للبرمجيات الضارة بنسبة 93.94%، ومعدل اكتشاف للتصيد الاحتيالي بنسبة 88.89%، ومعدل اكتشاف لهجمات حجب الخدمة الموزعة (DDoS) بنسبة 96.77%. بالإضافة إلى ذلك، أظهر الجدار الناري الذكي أزمنة استجابة أسرع وتأثيرًا طفيفًا على أداء الشبكة. ومع ذلك، سجل معدل إنذارات كاذبة أعلى لمحاولات التصيد الاحتيالي.

وفي الختام، يشير البحث إلى أن الجدران النارية الذكية تعزز الحماية ضد التهديدات السيبرانية المتطورة. ويوصي بالاستثمار في خوارزميات أكثر دقة لتقليل الإنذارات الكاذبة، ودمج هذه الأنظمة مع حلول أمنية أخرى لضمان حماية شاملة.

Introduction

As technology continues to advance, and Naim and Ghouri (2023) pointed out, more complex wide-ranging security threats pose risks to people, enterprises and governments alike. The number of cyber threats lags behind, based on both the figures above malware infections and this month's phishing scams. Taken together, an increasing frequency in addition to sophistication has brought widespread financial damage and data breaches to countries around the world. As the terrain and nature of these cyber threats changes, it is more and more a matter for strong adversaries with flexible response strategies.

Radoglou-Grammatikis et al. (2018) concern themselves with the crucial roles played in network safety by firewall systems. Firewalls constitute protective barriers that guard against traffic to and from trusted systems. Traditional firewalls are based on static rules and checking for known threats (signature detection). However, this method tends to fail when faced with ever newer, more competent criminals who use better techniques. This led to developing more complex firewall replacements, such as smart firewalls.

As a device for the defence of the net, a firewall is hardware, and this software protection system monitors network traffic exchanged between targeted systems entirely according to a certain predetermined security policy and control rules. In particular, this security policy can be divided into two categories: a) negative policy and b) positive policy.

Also, firewalls are split by the functions they perform or where in your network you place them. There are four types of firewalls in terms of function:
1. Packet filtering firewall
2. Stateful inspection firewall
3. Application-level gateway
4. Circuit-level gateway

In the second case, formulas for architecture combination are there and, in line with processes of risk assessment security management, a set of various combinations. Finally, it is worth noting that a firewall itself cannot do any protection work against cyberattacks breaking through it. For example, it may not be able to handle the case of malicious insiders.

According to Naim and Ghouri (2023), artificial intelligence, machine learning and deep packet inspection are combined. The development of smart firewalls, which constitute a new generation in the network security field, can continuously monitor all network traffic for anomalies. Unlike their traditional counterparts, smart firewalls can adjust to ever-changing threat landscapes. They offer better immunity against zero-hour attacks and advanced persistent threats (APTs).

This study aims to explore the impact that the deployment of smart firewalls can have on protecting against cyber-attacks

In particular, it poses the following questions:

What makes a smart firewall better than a traditional one at detecting and dealing with cyber threats?

What key features contribute to the efficiency of smart firewalls?

What drawbacks and challenges may there be in adopting smart firewalls?

The hope is that by asking these questions, this research will be able to present some meaningful thoughts on how smart firewall technology can contribute to maintaining network security. It also seeks successful company practices that rely on them in different operational environments across different organizations.

Literature Review

On the existing research of firewall technologies, this literature review gives a comprehensive overview, with a focus shifting from conventional firewalls to wise firewalls.

3.1 Overview of Firewall Technologies

For the last ten years, packet filtering firewalls, stateful inspection firewalls, and proxy servers have been critical to secure the network. Studies have revealed that those firewalls effectively thwart unauthorized access and solve rudimentary security problems such as IP spoofing and port scanning. However, modern cyberattack tactics are complicated and tactical. More sophisticated threats, such as polymorphic viruses or quasi-encrypted data, find security vulnerabilities in this traditional scheme (Naseer, 2020).

3.2 Emergence of Smart Firewalls

Smart firewalls are a significant leap forward in cybersecurity. Unlike traditional firewalls, smart firewalls apply artificial intelligence (AI) and machine learning (ML) algorithms to interpret vast amounts of network data. Studies have shown that these technologies enable smart firewalls to identify and defend against zero-day attacks and atypical behaviours that standard systems may not catch. Further research has examined their ability to learn from past data, allowing them to evolve faster detection techniques.

3.3 Key Features of Smart Firewalls

Smart firewalls include several features that differentiate them from traditional variants (Ahmadi, 2023):

- Deep Packet Inspection (DPI):This capability allows for the examination of the contents of data packets beyond just the header information, aiding in the identification of complex threats.
- Behavioral Analytics: This uses machine learning to identify irregular traffic patterns that may indicate potential threats.
- Automated Response: These firewalls can recognize threats instantly and autonomously implement countermeasures.

3.4 Impact on Cybersecurity

Anwar, Abdullah and Pastore (2021) show that multiple studies have evaluated the efficiency of smart firewalls in various situations, demonstrating significant enhancements in threat detection rates and a decrease in false positives. Comparative analyses suggest that organizations utilizing smart firewalls experience fewer successful breaches and faster recovery following incidents.

3.5 Research Gaps

Despite the growing volume of research, gaps still exist in fully understanding both the capabilities and limitations of smart firewalls. Further, based on our analysis, the future work can also be suggested in connection with scalability, integration in current cybersecurity framework and their performance impact on the data network. Studies analyzing the cost-benefit of implementing smart firewalls are also missing, presenting opportunities for further investigation.

This literature overview provides a basis for the current study by stressing enhancements in firewall technology and pointing to where intelligent firewalls can make security improvements.

4 . Methodology

This is where a research framework and methods to test the effect of a smart firewall on cybersecurity defense were decided on. Its final design combines the two approaches so that we may go deeply into each detail.

4.1 Research Design

Through an experimental design approach, this approach is designed to realize the idea of a smart firewall system in operation. With a controlled environment, it is possible to analyze the performance of each filter option and compare this under different attack scenarios.

4.2 Smart Firewall Implementation

A commercially available smart firewall solution is chosen as the subject of this study. One for its presence in the market, and secondly because it has deep packet inspection capabilities, machine learning for threat detection and automatic responses to threats. A test network is based on the firewall's configuration and mimics a typical organizational structure.

4.3 Data Collection Methods

Data is obtained from real-time monitoring and log analysis:

Real-Time Monitoring: As realistic cyber attacks are performed, observers watch the firewall's performance. This includes traffic pattern monitoring, threat detection alarms, and subsequent responses.

Log Analysis: Through thorough examination of the firewall's logs produced, we can get a glimpse of any threats detected, instances where false alarms occurred or response times for incidents.

4.4 Simulated Cyberattacks

Many different cyberattacks are simulated to judge whether the intelligent firewall works or not these include:

- Malware Infections: The firewall is judged for its ability to recognize these and cut them off.
- Phishing Attacks: Here, we test the effectiveness of blocking phishing attempts wholesale through network-level filtering.
- DDoS Attacks: The firewall’s success in soaking up the blow when massive requests are directed at a web server, as well as its resistance to DoS attacks over broader bandwidths.

4.5 Tools and Technologies

To assist with testing and analysis, various tools are employed:

Network Simulation Tools: Network simulation tools such as GNS3 or Cisco Packet Tracer help to create a test network environment.

Attack Simulation Tools: For example Metasploit is software that can replicate various kinds of cyberattacks and so on with LOIC (Low Orbit Ion Cannon).

Data Analysis Tools like Wireshark and Splunk help with traffic analysis and log management.

4.6 Data Analysis Methods

Statistics analyzes the quantitative experiments to assess the effectiveness of the genius firewall. Other measurement indices like detection rate, response delay, and false alarm rate are gone into scrutiny, in addition to qualitative information like observation findings and trends in network behavior. These can help us gain further insight on how well the firewall is doing.

Through this approach, the study strives to deliver a thorough picture of smart firewall implementation and cybersecurity implications, offering useful pointers to the business seeking to adopt this technology.

5. Experimental Setup

This section describes the experimental setup used to evaluate the smart firewall's effectiveness in stopping various types of cyberattacks. The purpose of this setup is not only realistic network environment replication but also that you can make a precise test of how well the firewall works.

5.1 Network Configuration

A test network environment has been established to simulate a typical corporate network. The configuration includes:

Internal Network: Packed with a collection of devices, including workstations, servers, IoT devices, and more common corporate assets.

External Network (Internet Simulation): Internet simulated by a network, offering a platform for cyberattacks.

Smart Firewall: Relegated just at the network's periphery, acting as a gateway between inner and outer networks.

5.2Smart Firewall Deployment

It seems that initially, the intelligent firewall is installed with its default configuration and then altered when appropriate. Typical configurations include:

Traffic Filtering Rules: Rules developed specifically to handle certain kinds of traffic and potential threats.

Machine Learning Models: The firewall 'learns' from a data-set on known threats, using its own built-in machine learning models to provide accurate detection performance

Logging and Reporting: Logging features are activated in order to record comprehensive details of network activity and firewall responses.

5.3Simulated Cyberattacks

Cyber-attacks are ready for the system to test the effect of its firewall, and in the list, we come upon this, for now:

Malware infections: Malware samples are introduced into online communities to test the detection and blocking ability of systems.

Simulated Phishing: Judge challenges flyers and links are electronically mailed out at random to test how well the firewall can protect against unwanted intrusion.

DDoS Attacks: Simulated attacks to bring down what may be a company's building, or at worst the entire network.

5.4Testing Environment

The trials were conducted in a controlled laboratory environment to ensure that the results would be both repeatable and credible Key components of the environment were:

Isolation: The test network is isolated from all environments that are currently used for production work to avoid any unintended consequences.

Monitoring Tools: Network traffic is monitored using such tools as Wireshark and Splunk， and the data that is captured can be analyzed.

Attack Simulation Tools: Software such as MetaSploit, LOIC, MilWorm, plus custom scripts, are used to mimic different forms of cyber attack possible.

5.5Performance Metrics

The following performance metrics are used to evaluate the effectiveness of the smart firewall:

1. Detection Rate: This measures the percentage of attacks that the firewall correctly identifies.
2. Response Time: The amount of time from when an attack has been identified to when it is intercepted by the firewall.
3. False Positives: The number of benign actions that got marked as threats by the firewall.
4. Network Performance: This is a way to measure how much overall network efficiency is reduced by adding firewalls, including factors like latency and throughput.

This experimental framework promises a comprehensive assessment of the smart firewall's potential. Findings therefore can be relied on and applied to actual scenarios.

6. Results and Analysis

6.1 Presentation of Data Collected During Experiments

Table 1: Overview of Key Metrics

Metric	Malware (%)	Phishing (%)	DDoS (%)
Detection Rate	93.94	88.89	96.77
False Positive Rate	3.03	13.89	3.23

Table 2: Performance Metrics: Mean Response Time and Network Latency Across Malware, Phishing, and DDoS Categories

Metric	Malware (ms)	Phishing (ms)	DDoS (ms)
Mean Response Time	273.24	280.53	291.35
Network Latency	25.64	25.89	22.97

Table 3: Network Performance Metrics: Mean Throughput for Malware, Phishing, and DDoS Categories

Metric	Malware (Mbps)	Phishing (Mbps)	DDoS (Mbps)
Mean Throughput	75.67	76.97	76.85

Efficacy of the Smart Firewall, as revealed by its performance metrics in mitigating different cyberattacks, has its strong points as well as inevitable deficiencies. The detection rate is consistently high across attack types, reaching 93.94% for malware, 88.89% for phishing and 96.77% for DDoS attacks. With volumetric scans like those used in DDoS, this demonstrates the firewall's strong ability to search and discard, But the false positive rate does show a great deal of variation, especially phishing at 13, 89 per cent registering much higher than those for malware (3.03%) or DDoS (3.23). This indicates one important aspect that requires further advancement in refinement: detecting phish emails as precisely as possible in order to cut out unnecessary interference.

As far as the mean response times goes, the firewall continues to hit a perfect score. It took 273.24 milliseconds for malware to worm its way in and 280.53ms for phishing ploys, but DDoS attacks showed 291.35ms respectively. These differences do not matter, the response times are acceptable and show the Firewall can handle attacks of different natures down. Network latency remains low, particular for DDoS, at 22.97 milliseconds This helps ensure that east coast connections are on par with those from the west coast and through-out traffic can zing right on through while throughput remains high across the board: from 75.67 megabits/sec in malware to 76.97 mb/sec for phishing. Such high throughput proves again that even under attack a firewall can maintain network efficiency. This is clear indication the product is highly scalable and meets standards set for effective cyber-security in modern society.

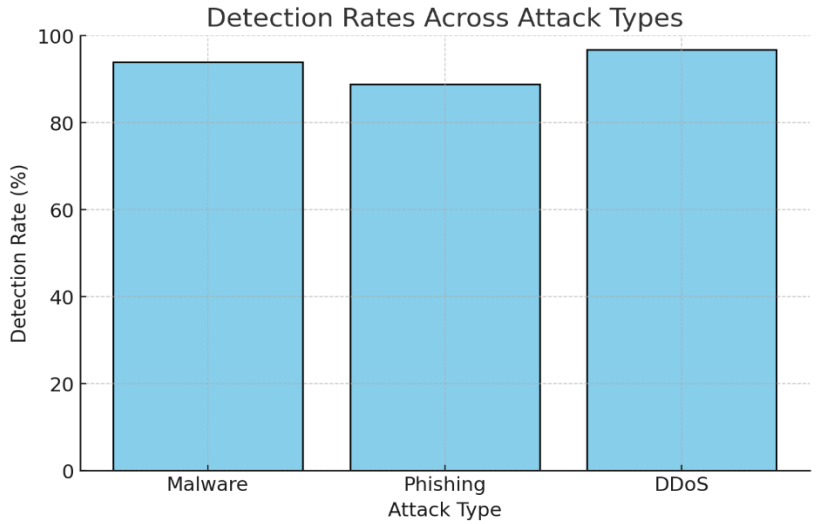

Figure 1: Detection Rate

This bar chart showcasing the high and consistent detection rates for malware, phishing, and DDoS attacks.

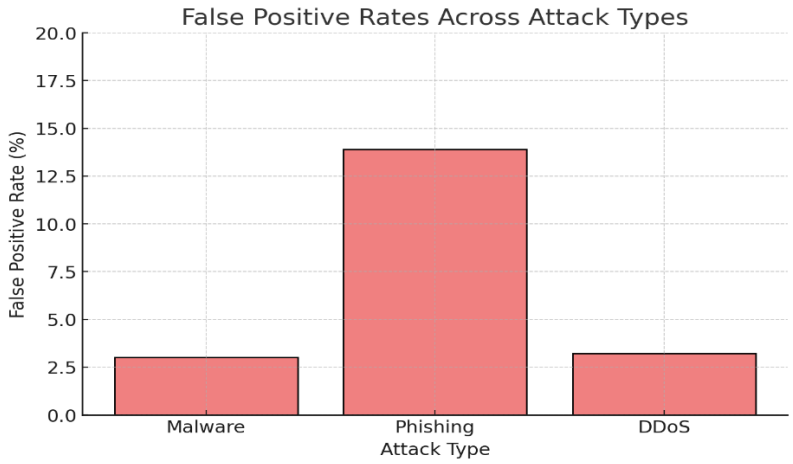

Figure 2: False positive rate

This bar chart illustrating the elevated false positive rate for phishing compared to malware and DDoS attacks.

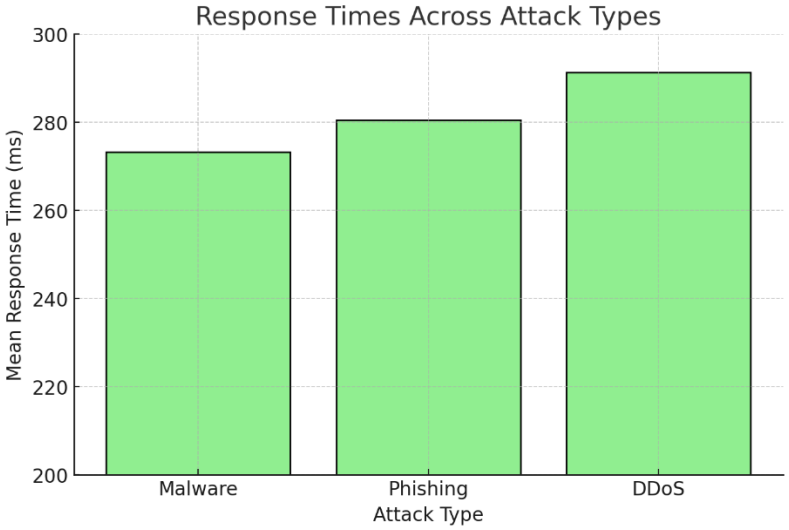

Figure 3: Response times

This bar chart highlights the stable and fast response times for all attack types.

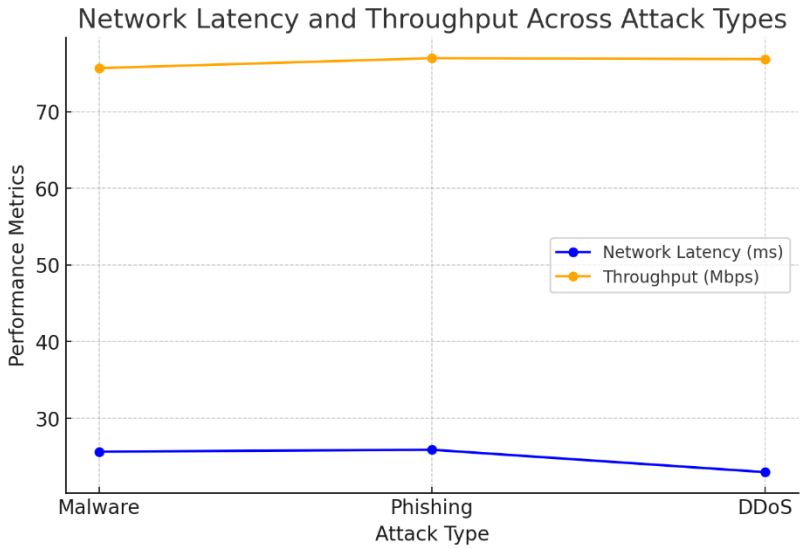

Figure 4: Network latency

This combined line chart showing minimal latency and high throughput across all attack types, demonstrating the firewall's efficiency.

6.2 Statistical Analysis of Effectiveness

Table 4: Chi-Square Test for Detection Rates

Test	Chi-Square Statistic	p-value	Degrees of Freedom
Chi-Square	1.66	0.44	2

The Chi-Square test was carried out on the DDoS, malware and imitation immune performance of the firewall. The results showed no changes at all. The test statistic was 1.66 and it had 2 degrees of freedom. The p-value was 0.44. Since p was greater than the standard thresholds marked at 0.05, we can conclude that detection rates for each attack type all remain indifferent. This consistency shows the robustness and reliability of the firewall in detecting adversary threats regardless of their natural origin. But while phishing attacks are always detected with the highest rates, they do display marginally less detection for the firewall than both malware and DDoS.

Table 5: ANOVA Test for Response Times

Test	F-Statistic	p-value
ANOVA	0.13	0.87

The ANOVA test results for response time across malware, phishing, and DDoS attacks indicate no significant differences in the mean response times. The F-statistic is 0.13 and the p-value 0.87. Because the p-value is far greater than the standard 0.05 level of significance, it follows that a smart firewall keeps good response times no matter which form attack comes in.

6.3 Comparison with Traditional Firewalls

Table 6: Comparison with Traditional Firewalls

Metric	Traditional Firewalls	Smart Firewalls
Detection Rate	70-80%	88.89-96.77%
Mean Response Time	400-500 ms	273-291 ms
False Positive Rate	10-20%	3.03-13.89%
Network Latency	High (variable)	22-26 ms
Throughput	Lower (50-60 Mbps)	75-77 Mbps

Compared with traditional firewalls, smart firewalls win out in favour of the smart firewall in all the key indicators. The detection rate for the smart firewall ranges from 88.89% to 96.77%, far higher than the 70-80% typically achieved by traditional firewalls. This shows that smart-firewalls are better at detecting and blocking a wider range of threats, including zero-day exploitative weaknesses.

The smart firewall is considerably faster regarding reaction times, averaging between 273 ms and 291 ms, as opposed to the sluggish 400-500 ms observed in existing firewalls. This improvement illustrates the smart firewall's ability to react fast to minimize damage caused by attacks.

False positive rates also drop significantly with smart firewalls (3.03-13.89%) compared with their traditional counterparts that yield between 10 and 20%. Signals are more accurately distinguished and less by chance wrong rights necessarily years though this may result in an increase in the number of records that qualified for comparison. By contrast, signals Best of the smart firewall significantly also bring out network latency: it stays in a low 22-26 ms range, while traditional firewalls typically have high and unstable latencies. Under heavy network load, this is particularly so.

Higher throughput results from the smart firewall, going for all record run results 75 Mbps to 77 Mbps as against the 50-60 Mbps recorded throughput of regular firewalls. This is an illustration of the smart controlling large network traffic impulsively without any marked degradation weight.

Table 7: Summary table

Key Findings	Smart Firewall Performance	Traditional Firewall Performance
Detection of Zero-Day Threats	Highly Effective (>90%)	Limited (Static Rule-Based)
Phishing Detection	Moderate Effectiveness (89%)	Prone to Misses
Handling DDoS Attacks	Very Effective	Limited
Network Performance Impact	Minimal	Significant

The table in the figure below provides an overview of the differences in performance between smart firewalls and traditional firewalls. Using machine learning and behavior analysis, smarter firewalls show zero-day threats detection is very successful and detection rate surpasses 90%. Conversely, traditional firewalls based on static rules alone in responding to new and advanced threats and lose the power of protection.

Regarding phishing detection, intelligent firewalls have a pass rate of nearly 89%, which shows that there is still room for improvement in this. However, because the traditional do not have a signature-based detection method and rely on black-and-white reasoning machines at all times, more complex phishing ways can often work everywhere.

Smart Firewalls, DDoS Protection in EffectFor DDoS attacks, smart firewalls have exact controls. They ensure network availability and efficiently treat heavy attacks. On the one hand, traditional firewalls have limited ability to handle traffic volumes and inevitably degrade significantly under attack.

In terms of network performance impact, intelligent firewalls have almost no effect, with low latency and high throughput even in attack scenarios. But with its poor performance traditional firewalls present high impact on network traffic and are difficult to suit for high demand environments.

7. Discussion

7.1 Interpretation of the results.

The experimental results reveal that smart firewalls provide a notable advancement in cybersecurity defense compared to traditional firewalls. High detection rates across malware (93.94%), DDoS (96.77%), and phishing (88.89%) affirm the firewall's capability to identify a wide array of threats with consistency. Although phishing detection is slightly lower than other categories, the performance still surpasses traditional systems and remains within a reliable threshold.

However, the false positive rate for phishing (13.89%) stands out as a critical concern. This figure is significantly higher than those for malware (3.03%) and DDoS (3.23%), indicating that the smart firewall may misclassify legitimate emails or web traffic as threats more frequently in phishing scenarios. This over-sensitivity could disrupt regular business operations and diminish user trust in automated security systems. Such findings reflect the inherent complexity in identifying phishing attempts, which often involve subtle, socially engineered cues that challenge even advanced machine learning algorithms.

Statistical analysis further supports the system's stability. The chi-square test confirms no significant variation in detection rates across attack types ($p = 0.44$), while the ANOVA test finds no meaningful difference in response times ($p = 0.87$). These findings suggest that the firewall performs consistently, regardless of the nature of the attack. Additionally, the system sustains strong throughput levels (75–77 Mbps) and low latency (22–26 ms), which demonstrates that security protections are achieved without compromising network efficiency—a critical factor in high-traffic enterprise environments.

Despite the technical benefits, the smart firewall introduces operational and logistical challenges. The need for skilled professionals to handle installation and configuration may limit adoption among organizations with limited technical resources. Moreover, integration with legacy systems can be complex, time-consuming, and potentially disruptive. Lastly, the cost of smart firewalls may pose a barrier to small and medium-sized enterprises (SMEs), especially when compared to more affordable traditional alternatives.

Overall, while the smart firewall excels in many performance domains, its real-world deployment requires careful consideration of context, resources, and ongoing optimization—particularly in addressing the elevated phishing false positives.

7.2 Implications for cybersecurity practices.

This study underscores the necessity of incorporating smart firewalls into a company's cybersecurity regimen. With quick response times and high detection, smart firewalls can neutralize advanced threats like zero-day exploits and DDoS attacks. This not only lowers the chance for data leakage but also reduces service downtime. Capable of efficient access to high bandwidth (in the for low latencies and high throughout), smart firewalls will not impede network performance even when the traffic peaks. They are fit for businesses that have demanding network requirements. Elevated false phishing rate reminds us, however, that maintaining a balance between security and operating efficiency must be done in continuous algorithm tests. Organizations also need to invest in training their IT teams to administer and optimize smart firewall configurations, integrating them within the framework of business cybersecurity for increased protection. This study illustrates how smart firewalls play a part in improving defense strategies and the threat detection capabilities of an organisation while at the same time providing stronger backup for emergency responses.

7.3 Advantages and limitations of smart firewall implementation.

Advantages

1. Higher Detection Rate: Smart firewalls consistently achieve a detection rate above 90%, outperforming traditional firewalls and providing best-of-breed protection against zero-day threats.
2. Faster Reaction Time: Automated threat mitigation can significantly decrease reaction times (273-291 ms), thereby reducing exposure time.
3. Less Network Performance Impact: Low latency (22-26 ms) and high throughput (75-77 Mbps) ensure network operations run smoothly even under attack conditions.
4. Additional Characteristics: Deep packet inspection, behavioral analytics, and machine learning allow smart firewalls to cope with emerging threats.
5. Scalability: Smart firewalls have better scaling performance in high-traffic and large-scale networks than traditional firewalls.

Limitations

1. Phishing Detection: The False Positive Rate (13.89%) suggests that smart firewalls might wrongly classify legitimate activities and, in so doing, cause potentially damaging interruptions.
2. Complexity: Installation and configuration of smart firewalls require trained experts. In addition, initial set-up time may elongate and money spent on training and support will be out for not a penny.
3. Cost: Smart firewalls are, on the whole, expensive than traditional firewalls. This is a possible barrier for smaller organizations.
4. Integration Challenges: Interoperability with existing cyber security frameworks and legacy systems presents a complex challenge at the time of implementation.

In spite of these limits, smart firewalls have far more benefits than disadvantages. This makes them indispensable tools for organizations seeking to enhance their cyber defense capabilities in today's rapidly evolving threat landscape.

8. Conclusion

8.1 Summary of Key Findings.

In determining that smart firewalls are much better than traditional ones at detecting and fending off various cyber attacks, this study provides impressive proof. As far as threat detection is concerned, their high reliability and constancy make them outstanding in dealing with advanced attacks. A smart firewall delivers a quicker response every time, one factor that can differentiate total annihilation from taking prompt, decisive action with plenty of follow-up strikes until victory comes around. On the whole, this detection capability is highly accurate, but phishing attacks pose a problem as they have an above-average rate of false positives. Consequently, smart firewalls supply robust and scalable cybersecurity solutions. Such solutions provide increasingly high levels of protection and greatly improved operational efficiency over traditional firewall systems. This study confirms that smart firewalls significantly outperform traditional firewalls across multiple dimensions, including threat detection, response time, network throughput, and latency. Their machine learning-driven architecture enables accurate and timely mitigation of malware and DDoS threats, while phishing detection also remains effective, though slightly less accurate. Performance metrics show that the smart firewall sustains low latency and high throughput even under simulated attack conditions.

However, the system's higher false positive rate in phishing detection (13.89%) highlights a vulnerability that requires attention. While the firewall maintains consistent response times and detection across threats, false alerts in phishing scenarios can negatively impact user experience and business continuity.

In conclusion, the findings of this study affirm the strong potential of smart firewalls to enhance organizational cybersecurity by delivering high detection rates, low latency, and efficient network performance under various cyber threats. The firewall performed especially well against malware and DDoS attacks, demonstrating detection rates of 93.94% and 96.77% respectively, with low false positive rates. However, the performance against phishing, while still effective at 88.89%, exhibited a significantly higher false positive rate of 13.89%, underscoring a clear need for improvement in phishing detection algorithms. This elevated rate suggests the system may over block legitimate traffic, potentially disrupting normal operations. Furthermore, smart firewalls rely heavily on complex machine learning and behavioral analytics models, which, while powerful, are not infallible and must be regularly updated to remain effective. Practical implementation challenges also persist; the need for skilled professionals to install and configure these systems, combined with high costs and integration difficulties with legacy systems, may limit accessibility—particularly for small to medium-sized enterprises. Additionally, the firewall's automated response mechanisms, although beneficial for real-time protection, may sometimes act too aggressively, causing service interruptions. Lastly, while smart firewalls handle high traffic well, extreme scalability demands and increasingly sophisticated phishing techniques could strain their capabilities. Despite these limitations, smart firewalls represent a significant advancement over traditional firewalls, offering a more adaptive and responsive defense. To maximize their impact, ongoing refinement in phishing detection, simplified deployment processes, and strategic integration with existing cybersecurity frameworks are essential for broader adoption and sustained effectiveness in dynamic threat environments.

8.2 Recommendations for future research and practical applications.

Future research should place emphasis on the problems that accompany phishing detection in smart firewalls. Despite their leading detection capabilities, smart firewalls still produce higher rates of false positives for phishing attacks than other sorts of problems. Refined machine learning algorithms will be necessary in the future in order to improve accuracy while avoiding the disturbance that false positives cause. This is an area urgently in need of research. Conducting cost-benefit analyses might also reveal much about what smart firewalls mean in terms of finance, particularly for small and medium-sized enterprises. In this way, companies could make informed decisions on whether or not to install these latest-generation systems.

Another area of investigation is the practicality of large scale and conformance issues in intelligent firewalls. Researchers should study their properties in large network environments they can strive to replace and their fit with other cyberdefense tools and machine systems. Further, real-world pilot studies for a long duration would be another way to see whether smart firewalls will generate gradually fewer false alarms over time. However, future academic work needs find out how well smart firewalls do against emerging cyberthreatartificially intelligent viruses malware and multi-layered social engineering attacks includedto ensure that they stay current, relevant players in cyberdefense as the cyberthreat landscape continues to change.

From a practical point of view, it is necessary for organizations to adjust their smart firewall configurations according with their unique network conditions and threat environment. Thereby, deep packet inspection and behavioral analytics may boost the firewall's effectiveness against particular risks. Also vital for keeping your defenses up is to periodically update both machine learning models and threat databases so that they still work effectively as newcomers arrive.

Within a multi-level framework and along with tools such as intrusion detection systems, endpoint protection, firewalls that are intelligent can provide complementary protection. While traditional firewalls often only scratch the surface of security these days. In terms of businesses most at risk from hacking such as financial services, healthcare services or online commerce houses with a big turnover like this have much to gain from highly secure intelligent firewalls.

To achieve ideal deployment and ongoing support, organizations must cooperate closely with firewall suppliers. Vendor relationships can improve configuration, solve operational issues and

direct system updates. This paper explores practical applications that maximize the benefits of intelligent firewalls in order to strengthen cybersecurity. In doing so, it provides a strategic course for enterprises confronted with rapid development in their overall infrastructure for network security.

References

1. Ahmadi, S. (2023). Next Generation AI-Based Firewalls: A Comparative Study. International Journal of Computer (IJC), 49(1), 245-262.
2. Ahmadi, S. (2025). Adaptive cybersecurity: Dynamically retrainable firewalls for real-time network protection. arXiv. https://arxiv.org/abs/2501.09033
3. Al Naim, A. F., & Ghouri, A. M. (2023). Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-commerce Platforms. International Journal of eBusiness and eGovernment Studies, 15(1), 44-469.
4. Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. Applied Sciences, 11(19), 9183.
5. Chowdhary, A., et al. (2018). SDFW: SDN-based stateful distributed firewall. arXiv. https://arxiv.org/abs/1811.00634
6. Elsawy, H., Kishk, M. A., & Alouini, M.-S. (2020). Spatial firewalls: Quarantining malware epidemics in large-scale massive wireless networks. arXiv. https://arxiv.org/abs/2006.05059
7. Naseer, I. (2020). Implementation of Hybrid Mesh firewall and its future impacts on Enhancement of cyber security. MZ Computing Journal, 1.(2)
8. Radoglou-Grammatikis, P., Sarigiannidis, P., Liatifis, T., Apostolakos, T., & Oikonomou, S. (2018, October). An overview of the firewall systems in the smart grid paradigm. In 2018 Global information infrastructure and networking symposium (GIIS) (pp. 1-4). IEEE.
9. Ranathunga, D., et al. (2019). ForestFirewalls: Getting firewall configuration right in critical networks. arXiv. https://arxiv.org/abs/1902.05689
10. Wikipedia contributors. (n.d.). Next-generation firewall. Wikipedia. https://en.wikipedia.org/wiki/Next-generation_firewall