Effectiveness of Next Generation Firewalls

Nathan Duc-Chuong Nguyen

Old Dominion University

ENGL 211C: Rhetoric, Writing, and Research

Professor Kevin Norris

April 15th, 2026

Abstract

Next generation firewalls (NGFWs) have become an important tool in modern cybersecurity as organizations face increasingly complex and frequent cyber threats. Traditional firewalls, which rely on static filtering and basic packet inspection, are often not sufficient to detect or prevent advanced attacks such as ransomware, malware, and unauthorized access. This study evaluates the effectiveness of NGFWs by analyzing existing research, industry reports, and benchmark testing data. A comparative secondary research method was used to examine key performance indicators, including threat detection rates, false positives and negatives, response times, and overall prevention success. The findings show that NGFWs significantly improve threat detection and response capabilities through advanced features such as deep packet inspection, intrusion prevention systems, and artificial intelligence (AI) based analysis. These technologies allow NGFWs to identify complex threats and adapt to evolving attack patterns more effectively than traditional systems. However, the study also finds that NGFWs have limitations, particularly in preventing attacks that rely on human error, such as phishing and credential theft. Overall, NGFWs are shown to be a highly effective cybersecurity tool, but they are most successful when used as part of a layered security strategy that includes additional protective measures.

Introduction

Every day businesses, hospitals, schools, and government agencies rely on digital networks to function properly. A single successful cyber attack can shut down operations, delay important services, freeze financial accounts, or expose sensitive personal information. In some cases, attacks on hospitals have even forced staff to delay critical medical procedures, showing how serious these threats can be. The impact of these attacks is not only financial but also affects

trust, safety, and reputation. As society becomes more dependent on technology, cybersecurity is no longer optional, it is necessary. At the same time, cyber threats such as malware, ransomware, phishing attacks, and unauthorized access continue to evolve, making them more difficult to detect and prevent using traditional security methods. Firewalls have traditionally been one of the most important tools used to protect networks. They act as a barrier between a trusted internal network and potentially harmful external traffic. However, traditional firewalls mainly rely on static rules, port filtering, and basic packet inspection, which are often not enough to stop modern cyber threats. Because of this, more advanced systems known as next generation firewalls (NGFWs) have been developed. These firewalls include features such as deep packet inspection, intrusion detection and prevention systems, endpoint aware inspection, and artificial intelligence (AI) based monitoring. These improvements allow NGFWs to analyze traffic in more detail, identify unusual behavior, and respond to threats more quickly than older systems. Even with these advancements, cyber criminals continue to find ways to bypass security systems. Attacks such as phishing and credential theft often rely on human error rather than technical weaknesses, which means they may not always be stopped by a firewall alone. In addition, many studies focus on explaining how NGFWs work instead of measuring how effective they actually are in real world situations. This creates a gap between what these systems are designed to do and how well they perform in practice. For organizations investing large amounts of money into cybersecurity, understanding this difference is extremely important. This study aims to evaluate how effective next generation firewalls are in preventing modern cyber threats such as ransomware, malware, and unauthorized access. By focusing on measurable factors like detection rates, response times, and prevention success, this research will provide a clearer understanding of how well NGFWs actually work. The goal is to determine whether these

advanced systems are as effective in practice as they are described in theory and to better understand their role in modern cybersecurity strategies.

Methodology

This study will use a comparative secondary research approach to evaluate the effectiveness of next generation firewalls (NGFWs). Instead of conducting original experiments, the research will rely on existing peer reviewed academic articles, cybersecurity industry reports, and independent benchmark testing results. Using secondary sources allows for the analysis of a wide range of data that has already been tested and validated, making it possible to compare results across different studies, industries, and testing environments. This approach also helps improve reliability by identifying consistent findings rather than depending on a single experiment. It also allows the research to include data from multiple perspectives, including both academic and industry based evaluations, which strengthens the overall analysis. The sources used in this study were selected based on their relevance to next generation firewall performance, their credibility as peer-reviewed or academic publications, and their focus on measurable cybersecurity outcomes such as detection rates and response times. The research will focus on several key performance indicators that are commonly used to evaluate cybersecurity systems. These include threat detection rates, false positive and false negative rates, response times to detected threats, and overall prevention success rates against attacks such as ransomware and advanced malware. Detection rates show how often a firewall correctly identifies a threat, while false positives and negatives help measure how accurate and reliable the system is. Response time is also important because faster detection and response can significantly reduce the damage caused by an attack, especially in time sensitive situations like ransomware infections. These metrics are widely used in cybersecurity research because they provide measurable and objective

ways to evaluate how well a system performs under pressure. Data for these measurements will be collected from laboratory simulations, penetration testing results, and independent benchmark comparisons between traditional firewalls and NGFWs. These sources often simulate real world cyber attacks to test how security systems perform under realistic conditions. By comparing multiple studies, this research will identify patterns and trends in firewall performance instead of relying on a single dataset. This makes the conclusions more balanced and applicable to real world scenarios. It also helps reduce the impact of any single study's limitations or biases. In addition to performance metrics, the study will also examine specific NGFW features such as deep packet inspection, intrusion prevention systems, endpoint aware monitoring, and artificial intelligence (AI) based analytics. These features will be analyzed to determine how much they contribute to improving detection and response capabilities. Understanding the role of these technologies will help explain why NGFWs may perform better than traditional firewalls in certain situations. Overall, this methodology focuses on measurable results rather than just describing firewall features. However, limitations such as differences in testing environments, variations in evaluation methods, and potential bias in industry reports will be considered when interpreting results. This approach will provide a clearer and more realistic evaluation of how effective next generation firewalls are in protecting against modern cyber threats.

Results

The results of this study show that next generation firewalls (NGFWs) are generally more effective than traditional firewalls across multiple performance metrics. NGFWs consistently demonstrate higher threat detection rates and lower false negative rates, meaning they are more successful at identifying real threats while minimizing missed attacks (Heino et al., 2022). This improvement is largely due to their ability to analyze network traffic at a deeper level using

technologies such as deep packet inspection, application awareness, and intrusion prevention systems. Unlike traditional firewalls, which rely mainly on static filtering rules, NGFWs are able to detect more complex and evolving threats, making them more reliable in modern cybersecurity environments. In terms of performance, NGFW systems maintain high levels of effectiveness even under heavy network traffic. Several studies report effectiveness rates above 94%, along with relatively low false positive rates, which indicates that these systems can accurately detect threats without significantly disrupting normal network activity (Hatkar et al., 2025). This is important because excessive false positives can reduce efficiency and create additional workload for security teams. The ability of NGFWs to balance accuracy and performance shows that they are capable of operating effectively in real-world environments where large volumes of data are constantly being processed. These findings also suggest that NGFWs can scale effectively in enterprise networks without major performance losses. The integration of artificial intelligence and machine learning also plays a major role in improving NGFW performance. Advanced detection models have achieved accuracy rates as high as 98%, demonstrating the ability of these systems to adapt to new and emerging cyber threats (Moila & Velempini, 2026; Zy et al., 2025). These technologies allow NGFWs to identify patterns in network traffic and detect anomalies that may indicate malicious activity. As a result, NGFWs are not only reactive but also proactive, allowing them to respond to threats more quickly and reduce potential damage. This level of adaptability is especially important as cyber threats continue to evolve at a rapid pace. However, the results also confirm that NGFWs are not completely foolproof. Attacks that rely on social engineering or human error, such as phishing, remain difficult to prevent using firewall technology alone (Watters, 2023). In addition, some advanced threats, including zero-day exploits and encrypted malware, may still bypass detection

systems. These findings highlight the importance of combining NGFWs with other security measures, such as user training, endpoint protection, and continuous monitoring. Overall, the results support the conclusion that NGFWs are a highly effective cybersecurity tool, but they must be used as part of a layered security approach to provide complete protection.

Discussion

Effectiveness of NGFWs

NGFWs demonstrate higher detection and prevention rates compared to traditional firewalls because they analyze network traffic in greater depth. Features such as deep packet inspection, application awareness, and intrusion prevention systems allow NGFWs to identify threats that would bypass basic filtering methods (Heino et al., 2022). In addition, research shows that NGFW systems maintain strong performance even under high network traffic, with effectiveness rates remaining above 90% in some testing environments (Hatkar et al., 2025). NGFWs are also more effective at detecting advanced malware and ransomware because they rely on behavior-based analysis instead of only predefined rules (Jenkinson, 2022). This allows them to identify suspicious activity even when threats attempt to disguise themselves as legitimate traffic. As a result, NGFWs significantly improve overall network protection and are considered a critical part of modern cybersecurity systems.

Advanced Technologies

One of the main reasons NGFWs are more effective is the integration of advanced technologies such as artificial intelligence (AI), machine learning, and automated threat detection. These technologies allow firewalls to continuously learn from new data and adapt to emerging cyber threats. For example, AI based models have achieved detection accuracy rates as

high as 95% to 98%, showing their ability to identify threats with a high level of reliability (Moila & Velempini, 2026). Machine learning techniques such as reinforcement learning and random forest models also improve the ability of firewalls to detect anomalies and predict attacks before they occur (Finistrella et al., 2025; Zy et al., 2025). These systems analyze patterns in network traffic and user behavior, allowing them to recognize unusual activity that may indicate a cyber attack. Additionally, modern NGFW systems integrate deep packet inspection with automated policy management, creating a more proactive and adaptive security system (Hatkar et al., 2025). This combination of technologies allows NGFWs to go beyond simple filtering and actively respond to threats in real time.

Limitations

Despite their advantages, NGFWs have several limitations that affect their overall effectiveness. One major limitation is their inability to prevent attacks that rely on human error, such as phishing and credential theft. Many ransomware attacks begin with user interaction, which means they can bypass firewall protections entirely (Jenkinson, 2022). In addition, cybercriminals continue to develop new techniques that can evade detection, including encrypted malware and zero-day exploits. This makes it difficult for even advanced systems to detect all threats in real time (Watters, 2023). Another limitation is that firewall performance can vary depending on testing environments and configurations. Some studies may also present biased results due to industry influence, which can affect the reliability of performance comparisons. Because of these limitations, NGFWs should not be viewed as a complete solution. Instead, they must be used as part of a layered cybersecurity strategy that includes user education, endpoint protection, and continuous monitoring.In addition to technical limitations, there are also real-world challenges that affect the implementation of NGFW systems. Deploying and

maintaining these firewalls can require significant financial investment, especially for smaller organizations with limited resources. In addition, NGFWs often require skilled cybersecurity professionals to properly configure and monitor them, which can increase staffing demands. Organizations may also face challenges when integrating NGFWs into existing systems, particularly if their infrastructure is outdated or not designed to support advanced security technologies. These factors show that while NGFWs are highly effective, their adoption can be limited by cost, complexity, and resource availability.

Conclusion

This study shows that next generation firewalls are significantly more effective than traditional firewalls in detecting and preventing modern cyber threats. By using advanced technologies such as deep packet inspection, intrusion prevention systems, and artificial intelligence, NGFWs are able to analyze network traffic in greater detail and respond to threats more quickly. The results demonstrate that these systems achieve higher detection rates, improved accuracy, and faster response times, making them a valuable component of modern cybersecurity strategies. However, the findings also make it clear that NGFWs are not a complete solution. Cyber threats that rely on human behavior, such as phishing and social engineering, can still bypass firewall protections. In addition, the effectiveness of NGFWs can vary depending on how they are implemented and the environment in which they are used. These limitations highlight the importance of using NGFWs as part of a layered security approach rather than relying on them alone. Overall, NGFWs play a critical role in protecting digital networks, but their success depends on how they are integrated with other security measures. Organizations must combine advanced technology with user awareness, proper configuration, and continuous monitoring to achieve the highest level of protection. As cyber threats continue

to evolve, future research should focus on improving adaptive security systems and developing more effective ways to address human related vulnerabilities.

References

Hatkar, S., Rout, K., Lad, A., & Swathika, O. V. G. (2025). An Integrated UTM Solution for Modern Cybersecurity: Combining Deep Inspection, ML, and Policy Automation. *IEEE Access*, *13*, 176010–176023. https://doi.org/10.1109/ACCESS.2025.3618281

Finistrella, S., Mariani, S., & Zambonelli, F. (2025). Multi-Agent Reinforcement Learning for Cybersecurity: Classification and survey. *Intelligent Systems with Applications*, *26*, Article 200495. https://doi.org/10.1016/j.iswa.2025.200495

Heino, J., Hakkala, A., & Virtanen, S. (2022). Study of methods for endpoint aware inspection in a next generation firewall. *Cybersecurity (Singapore)*, *5*(1), Article 25. https://doi.org/10.1186/s42400-022-00127-8

Jenkinson, A. (2022). Ransomware and Cybercrime (1st ed.). CRC Press. https://doi.org/10.1201/9781003278214

Moila, R. L., & Velempini, M. (2026). Integrating NLP and Ensemble Learning into Next-Generation Firewalls for Robust Malware Detection in Edge Computing. *Sensors (Basel, Switzerland)*, *26*(2), 424. https://doi.org/10.3390/s26020424

Turmudi Zy, A., Isarianto, I., Muhammad Rifa'i, A., Ghofir, A., Dwi Miharja, M. N., & Tri Sasongko, A. (2025). Optimizing firewall timing for brute force mitigation with random forests. *IAES International Journal of Artificial Intelligence*, *14*(4), 2945. https://doi.org/10.11591/ijai.v14.i4.pp2945-2954

Watters, P.A. (2023). Cybercrime and Cybersecurity (1st ed.). CRC Press. https://doi.org/10.1201/9781003406730

Reflection

AI Outline

I used the prompt Professor Norris showed us and entered my annotated bibliography into the AI tool to generate an outline. The output gave me a basic structure for organizing my paper, including sections that grouped my sources into major ideas. From there, it became a matter of adding my own information and adjusting the outline to better fit my research question. The AI helped me see how my sources could connect, especially when separating topics like effectiveness, technologies, and limitations. However, I did not follow the outline exactly as it was given. I made changes so it would better match the assignment requirements and flow more logically. For example, I organized my paper into Introduction, Methodology, Discussion, and Results, which made it easier to present my findings clearly. Overall, the AI tool was helpful for getting started and organizing ideas, but I still had to revise and build on it to make it fit my writing and argument.

Process

The writing process was easier since I already had my introduction and methodology completed before starting the full paper. Instead of starting from scratch, I focused on improving those sections by making them clearer and more detailed. I made small changes to wording, added more explanation where needed, and made sure they matched the direction of my research. When it came time to write the discussion and results sections, I mainly relied on my annotated bibliographies. Since I had already read and summarized my sources, it was easier to pull key information and connect ideas across them. The main challenge was not finding information, but organizing it in a way that made sense and did not repeat the same points too much. I had to focus on grouping similar ideas together and explaining them clearly. Overall, the process was

more about refining and organizing my research than starting new work, which made it more manageable.

Peer Review Integration

Peer feedback played an important role in improving my paper, especially in refining clarity, reducing repetition, and strengthening the overall depth of my analysis. One of the main suggestions I received was to reduce repetition in my introduction, specifically where I discussed the increase and advancement of cyber threats. In my original draft, I repeated similar ideas about cyber threats becoming more frequent and more advanced, which made that section feel slightly redundant. To address this, I revised those sentences to be more concise and combined overlapping ideas into a single, clearer statement. This helped improve the overall flow of the introduction and made it more engaging and easier to read. Another important piece of feedback was to better explain how I selected my sources in the methodology section. While I had described the types of sources I used, such as peer-reviewed articles and cybersecurity reports, I did not clearly explain the reasoning behind why those sources were chosen. Based on this suggestion, I added a sentence explaining that my sources were selected based on their relevance to next generation firewall performance, their credibility, and their focus on measurable outcomes such as detection rates and response times. This addition made my methodology more complete and gave readers a clearer understanding of how my research was conducted and why those sources were reliable. My peer also suggested that I include more real-world implications in my discussion section. Specifically, they recommended addressing factors such as cost, staffing requirements, and deployment challenges related to NGFWs. This was something I had not fully developed in my earlier draft. To improve this, I added a new paragraph to my limitations section that discusses the financial investment required to implement NGFWs, the

need for trained cybersecurity professionals to manage them, and the potential challenges organizations may face when integrating these systems into existing infrastructure. Including this information made my paper more practical and helped connect my research to real-world situations, rather than focusing only on technical performance. In addition to these major changes, I also reviewed my paper for smaller issues related to grammar and sentence structure. Although my peer did not identify any major errors, I still made minor corrections, such as fixing punctuation and improving sentence clarity. This helped make my writing more polished and professional. Overall, the peer review process helped me see my paper from a different perspective and identify areas that needed improvement. By applying the feedback I received, I was able to reduce repetition, strengthen my methodology, and add more depth to my discussion. These changes improved the clarity, organization, and overall quality of my paper while still maintaining my original ideas and writing style.