Title:
Evaluating the effectiveness of modern firewalls in preventing cyber threats: A Research Proposal

Name:
Nathan Nguyen

Institution:
Old Dominion University

Course:
ENGL 211C: Rhetoric, Writing, and Research

Instructor:
Professor Kevin Norris

Date:
February 23, 2026

Evaluating the effectiveness of modern firewalls in preventing cyber threats: A Research Proposal

Introduction

Everyday, businesses, hospitals, schools, and government agencies rely on digital networks to function. A single successful cyber attack can shut down operations, delay medical procedures, freeze financial accounts, or expose sensitive personal information. The damage is not only financial but also emotional and reputational. As society becomes increasingly dependent on interconnected systems, cybersecurity is no longer optional. Cyber threats such as malware, ransomware, phishing attacks, and unauthorized access have continued to grow in complexity and frequency. Firewalls are widely considered to be a primary line of defence against these threats. Traditionally, they acted as barriers between trusted internal networks and potentially harmful external traffic. However, modern firewalls, often referred to as next generation firewalls (NGFWs), have evolved to have deep packet inspection, intrusion detection, and prevention systems, endpoint aware inspection, and artificial intelligence (AI) based monitoring. Despite these advancements, cyber criminals continue to bypass security systems through sophisticated methods, especially social engineering and ransomware campaigns. This raises the question about how effective modern firewalls truly are in preventing contemporary cyber threats. As a cybersecurity major at Old Dominion University, I am particularly interested in evaluating whether foundational security tools like firewalls perform as effectively in practice as they are described in theory. This research proposes to evaluate the measurable effectiveness of modern next generation firewalls in preventing current cyber threats while identifying both their strengths and limitations.

Research Question

How effective are modern next generation firewalls in preventing contemporary cyber threats such as ransomware, malware, and unauthorized network intrusions.

Significance of the Study

With the increasing number of cyber attacks, organizations face pressure to balance limited cybersecurity resources with the need to protect sensitive data and maintain operational continuity. Investing in security infrastructure is costly, and decision makers must determine whether advanced firewall technologies provide measurable improvements over traditional systems. This study is significant for cybersecurity professionals, systems administrators, business leaders, and government agencies who depend on firewall technologies as part of their defence strategies. It is also relevant to everyday users whose personal information depends on organizational network security. By evaluating firewall effectiveness using measurable outcomes, this research can assist stakeholders in making informed decisions about cybersecurity investments and risk management strategies. Additionally, while many sources describe the features of modern firewalls, fewer studies directly compare their measurable performance against specific contemporary threats. This research seeks to address that gap by focusing on detection rates, response times, and prevention success rates rather than simply describing technological capabilities.

Literature Review

Recent academic research highlights the evolution of firewall technologies, (Heino et al., 2022), in the journal Cybersecurity (Singapore), examined methods for endpoint aware inspection in next generation firewalls. Their research explains how monitoring device behavior and network activity allows firewalls to detect suspicious traffic beyond traditional port and protocol filtering. This suggests that modern firewalls are more advanced than older systems because they analyze user and device behavior in addition to network traffic. However, while their study focuses on how these systems are designed and implemented, it does not directly measure how much more effective they are at stopping specific modern attacks compared to traditional firewalls. Other research has focused on improving cybersecurity tools through artificial intelligence (AI). (Finistrella et al., 2025), writing in *Intelligent Systems with Applications*, discusses how multi-agent reinforcement learning can improve threat detection systems over time. Their findings suggest that adaptive AI-based systems may respond better to evolving threats. Although this research highlights the potential benefits of machine learning in cybersecurity, it focuses more on system classification and theoretical models rather than measurable real world prevention rates. (Watters, 2023) explains that firewalls remain one of the most important tools in network security frameworks, but they cannot stop every type of cyberattack. He emphasizes that attackers often use social engineering to bypass technical defenses. Similarly, (Jenkinson, 2022) describes how ransomware frequently enters networks through phishing emails or stolen credentials, which may not always be intercepted at the firewall level.

Methodology

This study will use a comparative secondary research approach. Data will be collected

from peer-reviewed academic studies, cybersecurity industry reports, independent security benchmark testing, and documented simulation environments. Key performance indicators will include: threat detection rates, false positive and false negative rates, response times to detected threats, and prevention success rates against ransomware and advanced malware. Detection data will be gathered from laboratory simulations, penetration testing results, and independent benchmark comparisons between traditional firewalls and next generation firewalls. Additionally, firewall features such as deep packet inspection, intrusion prevention systems, endpoint aware monitoring, and artificial intelligence (AI) based analytics will be examined to determine their impact on measurable security performance. By focusing on quantitative performance metrics rather than solely descriptive features, this methodology will allow for a clearer evaluation of real-world effectiveness.

Expected Outcomes

It is anticipated that the next generation firewalls will demonstrate higher detection accuracy and improved response times compared to traditional firewall systems. Advanced features such as artificial intelligence (AI) assisted monitoring and deep packet inspection are expected to enhance protection against known malware and certain ransomware variants. However, the research may also confirm that firewalls alone cannot fully prevent attacks that exploit human vulnerabilities, such as phishing based credential compromise. The expected conclusion is that while modern firewalls significantly strengthen network defense, they must operate as part of a layered cybersecurity strategy to provide comprehensive protection.

References

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

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

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

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

Reflection on Process & Peer Review

During the peer review process, the most helpful critique I received was that my original introduction was informative but lacked urgency. While I clearly explained what firewalls are and how cyber threats function, a peer mentioned that the hook did not fully emphasize the real-world consequences of cyberattacks. In response, I revised my introduction to include specific examples such as hospitals being shut down, financial accounts being frozen, and sensitive information being exposed. This adjustment strengthened the pathos of my proposal by focusing on the human and societal impact of cybercrime rather than just technical definitions. By doing this, I made the topic feel more immediate and relevant to a broader audience. Another important suggestion was that my literature review summarized sources but did not clearly

identify the research gap. After reviewing that feedback, I revised the literature review to explain that while scholars discuss firewall architecture and artificial intelligence improvements, fewer studies directly measure comparative effectiveness between traditional and next generation firewalls against specific modern threats. This strengthened the logos of my proposal because it clarified why my research question matters within the academic conversation. Instead of simply reporting what other authors said, I now explain what is missing and how my research addresses that gap. Expanding the paper while maintaining a professional tone required me to add depth rather than repetition. I clarified how detection rates would be measured in the methodology section and identified stakeholders who would benefit from the findings. Since drafting my first version, my understanding of the research question has shifted from a general interest in firewall effectiveness to a focused evaluation of measurable performance against ransomware and malware. This revision process helped me better understand how rhetorical choices influence clarity, credibility, and overall persuasiveness.