Sentinel Wall Cyber Defence System

Aniket[1], Harshit Tiwari[2], Abhishek Yadav[3], Rimjhim[4], Akansha Rajput[5]

[1] Department of Computer Science and Engineering, Nitra Technical Campus, Raj Nagar, Ghaziabad, UP, India

[2] Department of Computer Science and Engineering, Nitra Technical Campus, Raj Nagar, Ghaziabad, UP, India

[3] Department of Computer Science and Engineering, Nitra Technical Campus, Raj Nagar, Ghaziabad, UP, India

[4] Department of Computer Science and Engineering, Nitra Technical Campus, Raj Nagar, Ghaziabad, UP, India

[5] Department of Computer Science and Engineering, Nitra Technical Campus, Raj Nagar, Ghaziabad, UP, India

Corresponding Author Email: aniketverma48986@gmail.com

Other Authors' Emails:
tiwariharshit98999@gmail.com, yadavabhirink@gmail.com, rimjhims9899@gmail.com

How to Cite this Article:

Rajput, A., Rimjhim, , Yadav, A., Tiwari, H. & Aniket, (2026). Sentinel Wall Cyber Defence System. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.936

https://doi.org/10.55041/ijcope.v2i4.936

Abstract

As the number of cyber attacks and other forms of internet-based hacking continues to grow exponentially every year, there is an increasing demand for new ways to secure networks efficiently and effectively while also being cost-effective and using as few resources as possible. Many conventional firewalls operate using pre-defined "rules," and do not provide real-time monitoring of any form so that they can quickly react to dynamic types of threats. The Sentinel Wall Cyber Defence System is a modular and light-weight firewall that has been specifically designed to monitor, analyze and control the traffic that flows in and out of a computer system/network in real-time using very little processing power/resources.

The system uses Scapy to capture and analyze packets, and iptables implements the security policies enforced at an operating system level. Sentinels will use a rule-based engine to process packets received based on pre-existing configurations defined in either JSON or YAML format to allow, drop, or log the traffic. To provide users with an easy to use interface to visually see network activity as it happens, a Graphical User Interface (GUI) has been developed that provides real-time monitoring of live network activity, as well as user activity on the network, and logs of all users that have been blocked from accessing any part of the network because they represented a threat to the network.

Results from testing indicate that the Sentinel Wall Cyber Defence System effectively filters unwanted network traffic, blocks unauthorized users from gaining access to the network, and uses very little processing power; thus providing a realistic, scalable method for improving network security, particularly in small or educational environments.

Keywords:
Cybersecurity, Personal Firewall, Network Traffic Analysis, Packet Sniffing, Rule-Based Filtering, Threat Detection, System Security, Network Monitoring

1. Introduction

The quick rise of digital communication, cloud computing, and devices that are connected to each other has made cyber threats much more likely. Malware infections, unauthorized access, phishing, and denial-of-service (DoS) attacks are just some of the attacks that modern systems are always open to. Most of the time, static rule sets are not enough for traditional firewall systems to find and stop advanced and changing threats. Because of this, there is a growing need for cyber defense systems that can adapt, work quickly, and work in real time.

The Sentinel Wall Cyber Defense System is meant to solve these problems by offering a firewall that is both light and strong. It uses packet sniffing, rule-based filtering, and real-time enforcement to keep an eye on and control network traffic. Scapy is used by the system to capture and analyze packets, and iptables is used to enforce rules at the operating system level. This combination makes sure that network communication is both visible and under control.

One of the main goals of the system is to keep a balance between security and performance. Sentinel Wall is different from heavy enterprise firewalls because it uses as few system resources as possible while still providing reliable protection. It works best for small networks, schools, and cybersecurity apps that are still in the testing stage. The system offers a useful way to make networks safer by combining monitoring and enforcement.

2. Literature Review

Over the years, cybersecurity research has changed a lot. It now focuses on things like intrusion detection systems (IDS), firewalls, and hybrid security models. Signature-based detection is used by traditional IDS tools like Snort and OSSEC. This works well for finding known threats, but it can't find zero-day or unknown attacks. Because of this limit, researchers have looked into using machine learning and artificial intelligence to find anomalies.

Recent studies show that AI-based intrusion detection systems work well to improve detection accuracy and cut down on false positives. IoT Sentinel and other systems show how behavioral analysis can be used to find strange patterns in network traffic, especially in IoT settings. Deep learning models are also used in cybersecurity to detect complex attack patterns that are hard to find with traditional methods. Modern cyber defense frameworks focus on automation, flexibility, and real-time response. Research shows that using multiple layers of security, such as monitoring, detection, and enforcement, leads to stronger protection. Hybrid systems that merge rule-based filtering with smart analysis are growing in popularity. The Sentinel Wall Cyber Defense System builds on these ideas by combining packet analysis with system-level enforcement. It mainly relies on rule-based filtering, but its modular design allows for future integration of smart detection methods. This makes it a flexible and scalable solution.

3. Methodology

The Sentinel Wall Cyber Defense System is built in a modular way that makes it easy to keep an eye on and control network traffic. The first step is to use Scapy, a powerful Python tool that can sniff and analyze network packets in real time, to capture packets. It gets important metadata like IP addresses for the source and destination, port numbers, and types of protocols.

Table 1: Packet Metadata Extracted

Field	**Description**	**Example**
Source IP	Sender IP address	192.168.1.10
Destination IP	Receiver IP address	8.8.8.8
Port Number	Communication port	80
Protocol	Type of protocol	TCP/UDP

Then, the rule engine uses predefined rules that are stored in JSON or YAML format on the extracted data. These rules set out what to do in certain situations, like letting certain types of traffic through, dropping them, or logging them. The decision module looks at each packet and decides what to do based on these rules.

When a decision is made, iptables is used by the enforcement layer to carry out the action at the operating system level. This makes sure that bad or unauthorized traffic is blocked right away, which is a good way to protect yourself. Additionally, the system has a graphical user interface (GUI) made with Tkinter that shows live traffic data, logs, and statistics for users to see.

The system's modular design makes it flexible, so that parts can be updated or replaced without affecting how the whole thing works. This method makes the system more scalable and able to handle future upgrades, like the addition of machine learning-based detection methods.

Figure 1:Dashboard Interface of Sentinel Wall System

Figure 1 shows the dashboard, which gives an overview of how well the system is working. It shows traffic stats, the number of allowed and blocked packets, and alert summaries. This makes it easier for users to interact with the firewall system and makes it easier to keep an eye on it.

4. Results

We tested the Sentinel Wall Cyber Defense System in a number of different situations to see how well it worked and how well it performed. The system worked well by letting safe traffic through, like DNS requests, and blocking unsafe or unauthorized protocols, like Telnet. IP-based filtering was also put in place, which made it possible to block only certain suspicious sources**.**

Table 2: Test Case Evaluation

Test Case	**Input Traffic**	**Expected Output**	**Actual Output**
DNS Request	Port 53	Allow	Allowed
Telnet Access	Port 23	Block	Blocked
Suspicious IP	192.168.x.x	Drop	Dropped

The logging feature worked well for keeping track of network activity, giving us useful information about traffic patterns and possible threats. The system also has a live traffic monitoring feature that shows real-time packet information like the source IP, destination IP, protocol, and action taken.

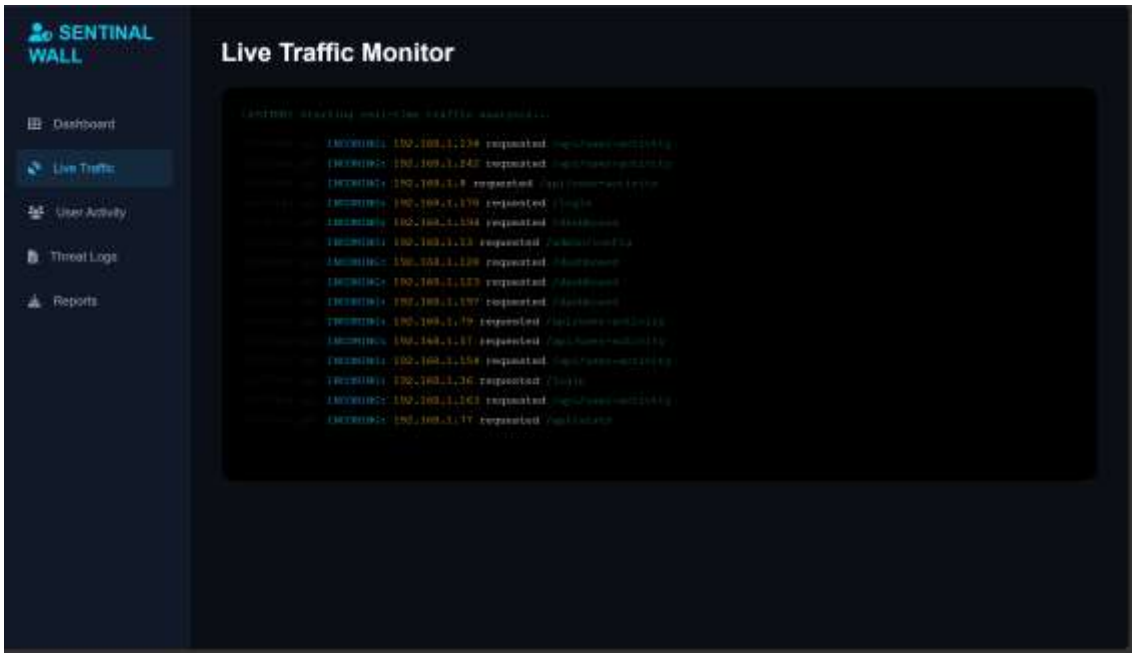
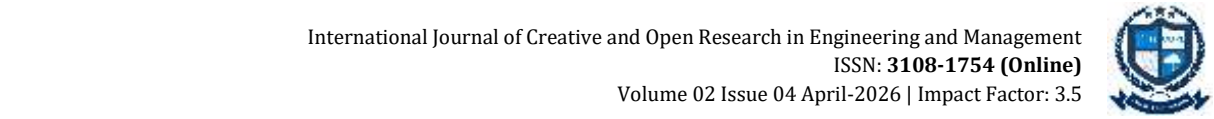


Figure 2:Live Traffic Monitoring Interface

As shown in Fig 2, the system captures and processes packets in real time, allowing users to clearly observe how each packet is handled (allowed, dropped, or logged).

The system does more than just monitor traffic. It also keeps track of what users are doing on the network. I think that helps in figuring out patterns in their behavior and how much they use it.



Like, understanding how people interact with everything there. And it picks up on stuff that seems off or unusual. That part is kind of important, but Im not totally sure how detailed it gets in practice.

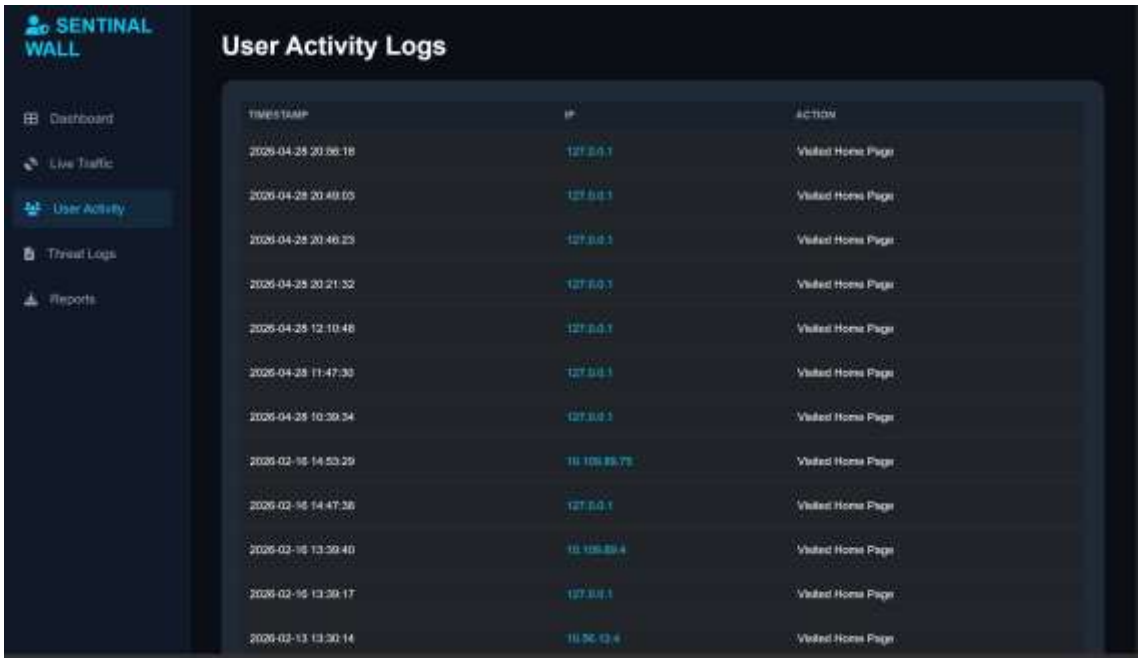


Figure 3: User Activity Monitoring Interface

Fig 3 illustrates the user activity module, which records interaction details and network usage, improving system transparency and behavioral analysis.

The system keeps these detailed logs on anything suspicious or when it blocks stuff. That way, people can go back and check them out for more analysis, or even for those forensic things. It seems like this really helps make the whole security part stronger overall. I am not totally sure, but logs like that probably catch patterns that might get missed otherwise.

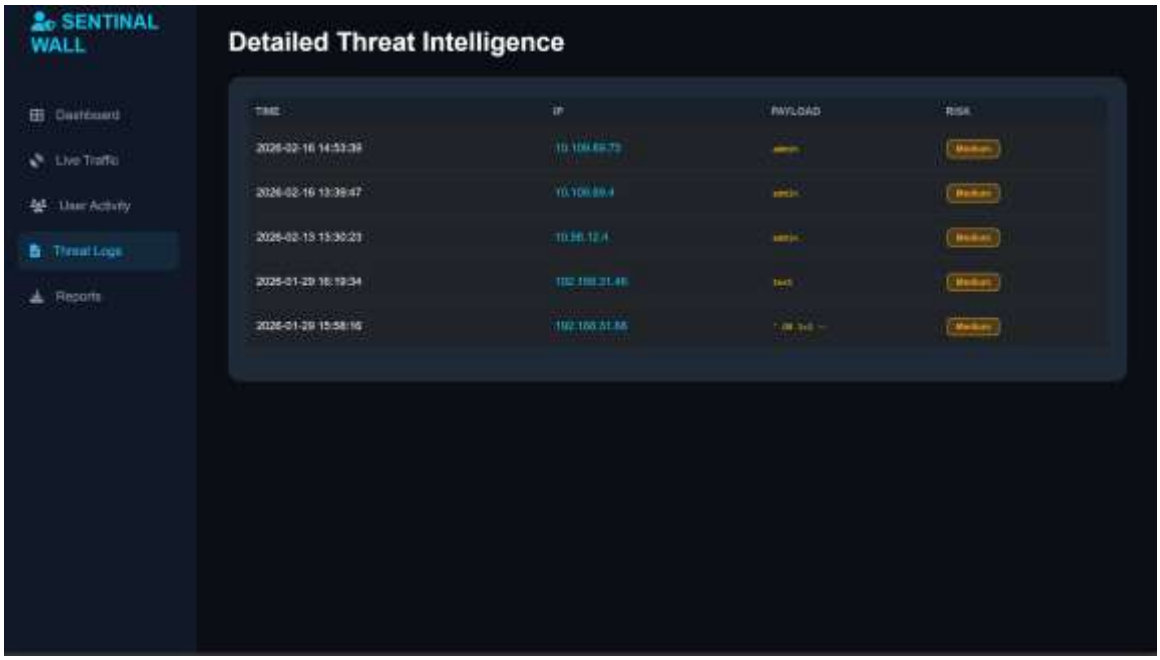


Figure 4:Threat Logs and Security Alerts

As shown in Fig 4, the threat logging module records all suspicious activities along with relevant details, helping in identifying and responding to potential cyber threats.

System performance evaluations demonstrate that the Sentinel system operates in an efficient manner using a minimum of resources due to its lightweight nature; thus, the system will not create a detrimental effect on system performance either. Therefore, it is a very suitable solution for deployment upon low resource devices. This system is able to perform real-time packet processing which gives you immediate assistance in detecting and responding to possible attacks.

The Sentinel Wall system provides you with improved visibility and flexibility in comparison with conventional firewall systems, through the ability to customize rules as well as monitor traffic in real-time; thereby giving you more access to the usability and effectiveness of the product. Based on these evaluations the system is recognized as a reliable and efficient means of basic network security.

5. Conclusion

The Sentinel Wall Cyber Defence System uses a more practical and efficient form of network security through the combination of analysis, monitoring, and implementation mechanisms. As opposed to the traditional firewall, which uses a static set of rules, Sentinel Wall offers real-time packet inspection and has the ability to implement security measures from the operating system level. This combined process allows for better detection and prevention of threats.

Scapy is used to perform detailed analysis of traffic patterns and inform the decision-making process using iptables for on-the-fly security enforcement. The addition of the graphical user interface (GUI) improves usability by providing instant access to network activity, while the system's lightweight design allows it to be utilized easily on smaller deployments and for educational purposes.

This project has shown that a well-architected and modular-based system can offer effective protection without needing excessive computational power. Combining rule-based filtering with real-time traffic monitoring enables improved visibility and control of all network traffic.

Overall, this project emphasizes the need to integrate different forms of security technology into one complete cyber defence system. This project will form a significant base for the future of network security research and development.

6. Future Scope

There is much room for further enhancement and development of the Sentinel Wall system. One of the enhancements involves using Machine Learning Algorithms for Anomaly Detection. Incorporating machine learning into the Sentinel Wall system would allow the system to find unknown threats and adjust to new attack patterns instead of using rule-based detection.

Another enhancement would be automating the process of automatically generating rules based on traffic behaviour. This improvement will decrease the amount of time required to configure rules manually while improving overall efficiency

Additionally, adding support for nftables to the Sentinel Wall System will make it more flexible and current. Cloud-based monitoring and remote access features would provide better scalability and ease of use for users trying to manage from different locations.

Integrating with an SIEM (Security Information and Event Management) System would allow for central logging, as well as increased capability for analysing the logs recorded by the Sentinel Wall system.

Implementing the Sentinel Wall System as a background service would enhance ease of use and allow for a greater level of automation.

Further research should include potential uses of Threat Intelligence Feeds and real-time updates to improve detection accuracy. These enhancements will allow for the transformation of the Sentinel Wall, creating a more enterprise-level and advanced Cyber Defence Solution.

Acknowledgement

We would like to express our sincere gratitude to our project guide and faculty members for their continuous support, valuable guidance, and encouragement throughout the development of this project. Their insights and suggestions greatly contributed to the successful completion of the *Sentinel Wall Cyber Defence System*.

We also extend our thanks to our institution for providing the necessary resources, infrastructure, and learning environment to carry out this work effectively.

Finally, we would like to thank our peers and team members for their collaboration, cooperation, and constructive feedback during the project development and research process. Their contributions played an important role in refining and improving the system.

References

[1] W. Stallings, Cryptography and Network Security, 7th ed., Pearson, 2017.
[2] W. Stallings, Network Security Essentials, Pearson, 2014.
[3] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” 2018.
[4] M. Roesch, “Snort: Lightweight Intrusion Detection,” USENIX, 1999.
[5] OSSEC, “Host-Based Intrusion Detection Guide,” 2020.
[6] V. Paxson, “Bro: A System for Detecting Network Intruders,” Computer Networks, 1999.
[7] S. Miettinen et al., “IoT Sentinel,” IEEE ICDCS, 2017.
[8] A. Javaid et al., “Deep Learning for Network Intrusion Detection,” IEEE, 2016.
[9] Y. Xin et al., “Machine Learning for Cybersecurity,” IEEE Access, 2018.
[10] A. Patcha and J. Park, “An Overview of Anomaly Detection,” Computer Networks, 2007.
[11] Linux Netfilter Project, “iptables Documentation,” 2022.
[12] Scapy Documentation, “Packet Manipulation Tool,” 2023.
[13] OWASP Foundation, “Top 10 Web Security Risks,” 2021.
[14] Cisco, “Cybersecurity Whitepaper,” 2022.
[15] Symantec, “Internet Security Threat Report,” 2021.
[16] Kaspersky, “Cyber Threat Intelligence Report,” 2022.
[17] IEEE, “Intrusion Detection Systems Research Papers,” 2020.
[18] ACM Digital Library, “Cybersecurity Studies,” 2021.
[19] Springer, “Advances in Cybersecurity,” 2022.
[20] R. Sommer and V. Paxson, “Outside the Closed World,” IEEE S&P, 2010.
[21] G. Creech and J. Hu, “Behavior-Based Intrusion Detection,” IEEE, 2014.
[22] S. Axelsson, “Intrusion Detection Systems: Survey,” 2000.
[23] MITRE, “ATT&CK Framework,” 2021.
[24] ENISA, “Threat Landscape Report,” 2022.
[25] IBM, “Cost of a Data Breach Report,” 2023.