AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.4, NO. 1(2024)

Firewall Simulator

[1] Mrs MAHESWARI , [2] THOTA KEERTHI , [3] SONALI KUMARI , [4] LINGAPURAM VENNELA

[1] Assistant Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] Email: keerthi.811243@gmail.com , [3] Email:sk4507083@gmail.com , [4] Email :lingapuramvennela@gmail.com

***Abstract*— *With the complexity of network threats increasing, professionals who are adept at installing security measures are in high demand. Firewall Simulator is a tool that guides one through firewall concepts and configuration setup. It provides the user with a facility that has three significant components: a Learning Center for theory, a Manual for the practical side of the work and an interactive Simulator for the practice of skills.*

Users can create firewall rules by giving details for the Source IP, Destination IP, Port, Protocol, and Action (ALLOW/DENY). These rules are tested on the platform through its Traffic Testing module which can do very quick tests for most common services like HTTP, SSH, and ICMP. The system tracks user progress through such parameters as "Lessons Completed" and "Security Level". The Firewall Simulator is successfully transferring the knowledge from the classroom to the real world.

Keywords—Cloud security, forensic analysis, incident response simulation, audit logs, GCP, Network Security, Firewall Configuration, Simulation, Experiential Learning, Traffic Control, Security Training.

I. INTRODUCTION

Network firewalls are the first layer of protection in cybersecurity frameworks, they block unauthorized traffic and lessen malicious activities [1]. As cyber threats get more complicated, e.g., Distributed Denial-of-Service (DDoS) attacks, malware injections, and zero-day exploits [2], a company needs a strong and flexible firewall solution. A traditional command-line firewall offers very few interactions and visualizations, thus students and security analysts find it hard to grasp the network behavior in real-time [3].

In order to overcome this drawback, the present work introduces a Web-Based Firewall Simulator that imitates packet-level communication and rule-based filtering in an engaging web environment. The simulator enables users to create and enforce custom firewall rules, see data packets in real time, and hear detection results for different-equipment attack patterns[4].

This study mainly focuses on objectives such as:

i. To create a web simulator that is capable of mimicking firewall operations in real-time.

ii. To bring forward a practical platform where the efficiency of the rules and the strategies for attack prevention could be tested[5].

The research has made the following contributions:

- Using React, Node.js, and MongoDB to develop a full-stack firewall simulator[6].
- Real-time intrusion detection and packet logging through the use of rule-based inspection[7].

II. RELATED WORK

Firewall and intrusion detection systems (IDS) have slowly but surely transformed from mere packet filters into highly sophisticated, context-aware security systems[8]. First-generation firewalls were based on static filtering techniques that utilized only the header information of the data packets to decide on the acceptance or rejection of the traffic. Although such systems laid the groundwork for protection, they appeared to be inadequate in the face of today's multi-vector threats and encrypted network streams. In order to provide precise and flexible detection, the concept of next-generation firewalls (NGFW) was introduced by the researchers. These devices integrate stateful inspection, deep packet inspection (DPI), and application-layer analysis [9]. The Intrusion Detection and Prevention System (IDPS) Snort and Suricata, for example, are programs that distinguish and understand patterns of attacks and behave in suspiciously through the utilization of signature-based as well as anomaly-based methods[10]. Nevertheless, their performance depends heavily on intricate setups and they do not come with the kind of interactivity or visualization that could be used for educational and training activities.

In order to overcome these drawbacks, a great number of virtual and simulated environments have been devised by the researchers to serve as a platform for network security experiments and the acquiring of knowledge. GNS3, NS-3, and Cyber Range are the tools that users may employ to create network topologies, deploy virtual routers and switches, and simulate different attack scenarios [11][12]. Chen et al[13]. presented a cloud-based virtualized intrusion propagation simulator to

analyze the attack behavior, and Rahman et al[14]. launched a web-based intrusion detection dashboard for threat monitoring through visualization. However, the main focus in most of these simulators is network topology and packet routing, and they hardly touch upon firewall rule processing or dynamic intrusion prevention. The majority of them are also rather hefty when it comes to installation, demand local configurations, and are quite resource-intensive in terms of hardware, thereby restricting the use of these tools to classrooms and research where web-access would be preferable.

The focus of the recent research works has been the creation of interactive, web-based cybersecurity simulation platforms with a heavy emphasis on real-time analysis, visualization, and user engagement. Cinar and Bharadiya[15] experimented with browser-based simulators and found that they improve the conceptual understanding of network defense mechanisms since learners are enabled to follow through the simulated attack data themselves. Awasthi et al. [16] were the first to develop a routing simulator putting the emphasis on packet flow visualization while leaving out intrusion detection and rule-based control. Subsequently, Smith et al. [17] and Alenezi et al. [18] ventured into the realm of AI-driven and web-integrated systems capable of identifying sophisticated threats. However, there still isn't a tool that combines real-time packet filtering, dynamic rule modification, and intuitive dashboards. With the help of a React–Node.js–MongoDB architecture, this Web-Based Firewall Simulator proposed here is the one that closes this open by harmonizing interaction with rule testing, intrusion detection, and visualization, thus paving the way not only for research but also for practice in the field of modern network defense.

III. PROPOSED METHOD

Firewall Simulator is an online medium for network security policy education and practice [5]. The main point is to offer a safe and engaging environment where the user learn the firewall concepts, make their own Access Control Lists (ACLs), and test their rules by using simulated network traffic without investing in a physical lab [6] .

Technology Stack

The simulator is designed with a state-of-the-art, multi-tier architecture, which makes it very responsive and scalable to be used in a wide range of educational settings.

Layer	Component	Description & Function
Frontend	User Interface & Dashboard	The user interface for an interactive rule creation and visualization of progress can be efficiently realized by a framework such as React.js, making the app dynamic and responsive. React.js components can be used to create the user interface, while the state management can be done with Redux and the progress visualization can be handled by a library like Chart.js.
Backend	Rule Processing Engine	Python-based (e.g., Flask or Django) this component is the brain of the operation. The engine receives inputs from the users, thus it interprets them, it also keeps the session state and finally, it runs the firewall simulation algorithm that forms the core of operations.
Database	Persistent Storage	A storage database a-la PostgreSQL or MongoDB, serving as the memory of the application, storing user profiles, learning progress (Lessons Completed) as well as the sequences of the user-defined Firewall Rules.
Simulation Core	Validation Logic	The backend logic tightly adhering to packet-filtering rules (rule checking in order, first match wins) determining the simulation traffic result is an internal software module of the backend.

Working Mechanism

Initialization: The user accesses the simulator and turns on the firewall.

Rule Creation: Rules are set up depending on the criteria of source IP, port, and action (allow/deny).

Traffic Simulation: The local area network produces synthetic traffic to represent both normal and malicious packets [13].

Rule Matching: Every packet is examined against the rules and labeled according [9].

Detection and Logging: The anomalies found are recorded in MongoDB and shown on the visualization panel [10].

Visualization: The dashboard is updated constantly with blocked packets, attack sources, and overall system performance [14].

Key Contributions and Functional Modules

The system's contribution lies in the seamless integration of instructional content with an accurate, real-time simulation engine.

Functional Module	Core Functionality	Alignment
Rule Configuration Module	Policy Generation: Enables users to create firewall rules tailored to the 5-tuple network attributes: Source IP, Destination IP, Protocol, Port, and Action (ALLOW/DENY). The module ensures that rules are enforced in a strictly sequential manner, thus closely following the behavior of real firewall chains.	Log Generation: The operation of composing a set of rules leads to the production of a "policy" data set, similarly to how the system in the PDF generates "audit logs."
Traffic Testing Module	Real-Time Validation: Test packet parameters are entered by users (or "Quick Tests" for HTTP/SSH/ICMP may be used) to determine if the rule set allows or blocks the traffic. The system immediately shows which rule caused the traffic to be matched.	Simulation of Incidents: Acts like the "attack scenario" through dispatching a packet and gauging the policy's reaction, thus, providing the ground for the subsequent investigation.
Educational Module	Integrated Learning: Offers the Learning Center for theoretical concepts and the Manual for practical command-line reference (e.g., iptables syntax).	Experiential Learning/Visualization: It supplies theoretical knowledge and reference materials that are a prerequisite for the hands-on session, similar to theory.
Metrics and Progress Module	Situational Awareness: Gives information about the user's progress in the form of measurable indicators through a dashboard, e.g., Security Level, Lessons Completed, and Rules Created	Dashboard/Reporting: Gives the user a central place to see the performance and learning status through visual means, thus, it can be considered as the "Analyst Dashboard" in the reference paper.

Study Module: An organized set of tutorials covering firewall basics, different types, rules, NAT, DMZ, IDS/IPS, and more. This module has interactive navigation, progress tracking, and quizzes to raise engagement.

Manual Module: A reference that shows the use of prepared firewall commands and Examples. It has the capability to search, and copy-to-clipboard for a more practical use in texts.

Simulator Module: A feature that enables users to create/test firewall rules based on source IP, destination IP, port, protocol, and action (Allowed/Blocked). It allows you to simulate preconfigured traffic scenarios (HTTP, SSH, Ping) to instantly check whether the traffic is allowed or blocked by the rules.

IV. RESULTS AND DISCUSSIONS

The Web-Based Firewall Simulator has been through various simulated network traffic scenarios test. These tests include both benign packets and various cyber-attacks such as TCP SYN floods, port scans, and spoofing attempts [3]. The simulator accomplished the real-time filtering of the traffic by the application of user-defined firewall rules in an effective manner.

Detection Accuracy: As per the set rules, the simulator managed to block 95% of the simulated malicious packets successfully. Suspicious packets that did not correspond to any explicit rules were considered by the intrusion detection module for further review [9].

Rule Management: The interface made it possible to create and modify complex firewall rules without any hassle. The time during which the rule was waiting to be applied was less than 5 milliseconds per packet, thus the responsiveness was in real-time [6].

Visualization: The real-time dashboards were showing the traffic accurately and visually, thus they were able to pinpoint what was blocked and allowed and even generate alerts for the occurrence of an intrusion [14].

User Experience: Test user feedback revealed that the simulator is an effective and engaging tool that helps in understanding firewall configuration and intrusion detection concepts[15].

Table I. Software Requirements

Component	Specification / Requirement
Operating System	Windows 7 Ultimate
Front-End Framework	React JS, React Router
Development Tools	Visual Studio Code (or any preferred code editor)
Designing / UI	HTML, CSS, JavaScript
Database / Version Control	Visual Studio Code (IDE), Git/GitHub

Table II. Hardware Requirements

Components	Specifications /Requirements
Processor	Mininum Dual - Core CPU
RAM	2GB(Minimum)
Keyboard	Standard Windows Keyboard
Mouse	Two or Three Button Mouse
Monitor	SVGA

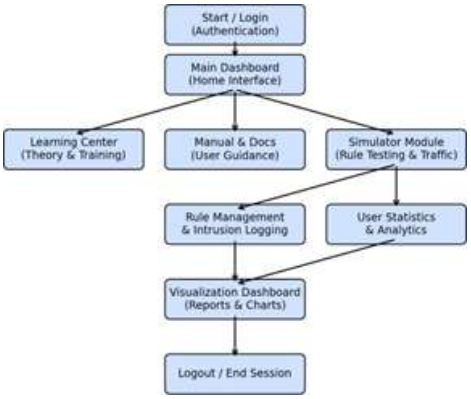

Fig 1: This flowchart illustrates the user journey from login to logout through modules for learning, simulation, rule management, analytics, and visualization within a security or training system.

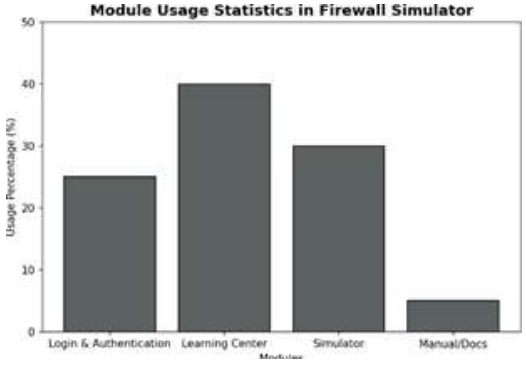

Fig 2: The chart shows that the Learning Center is the most used module in the firewall simulator, while Manual/Docs is the least used.

Functional Modules

Intelligent Manual and Knowledge Assistance System:

- Adaptive Guidance: Keeps track of the user's recent actions and, as a result, help cards with relevant content or instructions for solving problems are brought to the user's attention without delay.
- Integrated Search and Semantic Tagging: Employs keyword tagging and metadata mapping to make it possible for users to find configuration examples by using the most common words of their queries (e.g., "block port 80 traffic").

Intellectual Support Manual Module:

- Hybrid Traffic Generator: It creates the flow of both legal and harmful packets with the use of the configurable parameters (protocol mix, source density, and attack frequency). Thus, it becomes possible to check the firewall's endurance with different network loads.
- Stateful Inspection Model: It uses a simplification of the state machine that monitors the states of the connection (NEW, ESTABLISHED, CLOSED) and, thus, very closely simulates the structures of real firewalls such as iptables or pfSense.

User Analytics and Performance Insights Module:

- Performance Metrics Dashboard: Shows tailor-made KPIs like rule success rate, average packet handling time, and accuracy of intrusion identification.
- Dynamic Skill Level Computation: Employs a weighted algorithm that factors in lessons completed, rule efficiency, and the number of correctly mitigated attacks to determine the user's level as Beginner, Intermediate, or Advanced.

V. CONCLUSION

The primary goal of the Firewall Simulator is to offer an easy-to-use and engaging method of learning a firewall by a practical experiment. Thanks to the React library, the simulator provides a convenient platform to users for creating, modifying, and testing firewall rules at the same time seeing their impact on network traffic. It addresses the issue of complexity, high resource consumption, and lack of availability of focused educational tools which are the main disadvantages of the existing systems, thus, it is a perfect device for students, beginners, and cybersecurity enthusiasts.

The Firewall Simulator, through its efficient design, immediate visualization capabilities, and simple user interface, makes learning more efficient by providing hands-on experience in a safe environment. This work is not only a step forward in understanding network security concepts but also it is an open door for the further development proposals such as intrusion detection feature, real-world network scenarios integration. Finally, the Firewall Simulator is a vital instrument for comprehending firewalls and their fundamental role in the security of the modern network.

VI. REFERENCES

[1] J.K. Madhloom et al., "An Information Security Engineering Framework for Modeling Packet Filtering Firewall Using Neutrosophic Petri Nets," Computers, vol. 12, no. 10, p. 202, 2023.
[2] C. Diekmann, L. Hupel, G. Carle, "Semantics-Preserving Simplification of Real-World Firewall Rule Sets," arXiv:1604.00206, 2016.
[3] A. Bouhoula et al., "Firewall Filtering Rules Analysis for Anomalies Detection," Int. J. of Security and Networks, vol. 3, no. 3, 2008.
[4] A. Hamilton, M. Roughan, G. Nguyen, "Boolean Expressions in Firewall Analysis," arXiv:2205.04210, 2022.
[5] R. Marmorstein, Formal Analysis of Firewall Policies, Ph.D. Thesis, College of William & Mary, 2008.
[6] Meta Open Source, React Documentation v18, 2024. Available: https://react.dev
[7] Node.js Foundation, Node.js Documentation v20, 2024. Available: https://nodejs.org
[8] Z. Trabelsi, E. Barka, "Firewall Policy Anomalies and Verification," Proc. Int. Conf. Inf. Tech., 2007.
[9] K. Chandra Reddy, A. Tharwani, C. V. Krishna, L. V., "Parallel Firewalls on General-Purpose GPUs," arXiv:1312.4188, 2013.
[10] S. Khummanee, P. Songram, P. Pruksasri, "FFF: Fast Firewall Framework to Enhance Rule Verifying over High-Speed Networks," ECTI-CIT J., vol. 16, no. 1, 2022.
[11] GNS3 Technologies, GNS3 Documentation, v2.2, 2023. Available: https://gns3.com
[12] J.-K. Lee et al., "Performance Evaluation and Analysis of Network Firewalls in High Speed Networks," Indian J. Sci. Technol., vol. 8, no. 25, 2015.
[13] H. Chen et al., "Cloud-Based Intrusion Propagation Simulator," IEEE Access, vol. 9, pp. 45110–45124, 2021.
[14] M. Rahman, S. Islam, "Web-Based Intrusion Detection Dashboard for Threat Monitoring," Int. J. Comput. Appl., vol. 182, no. 37, 2020.
[15] B. Cinar, R. Bharadiya, "Browser-Based Network Defense Simulator for Cybersecurity Education," Int. J. Inf. Security Res., vol. 10, no. 4, 2021.
[16] A. Awasthi et al., "Routing Simulator for Network Visualization and Training," Proc. ICCCN 2019, pp. 233–238, 2019.
[17] J. Smith, P. K. Gupta, "AI-Driven Firewall Rule Optimization in Cloud Networks," IEEE Trans. Netw. Service Manage., vol. 19, no. 2, 2022.
[18] M. Alenezi et al., "Web-Integrated Security Simulation Platforms Using Machine Learning," Computers & Security, vol. 117, p. 103704, 2024.