RIPHAH INTERNATIONAL UNIVERSITY

Faculty of Computing
FINAL YEAR PROJECT PROPOSAL & PLAN

NeuroWall

Project Team

Full Name of Student	SAP Id	Program	Contact Number	Email Address
Muhammad Ubaid Ullah	32602	BSCY	0319-0978119	32602@students.riphah.edu.pk
Hamza Gulzar	31621	BSCY	0311-5448009	31621@students.riphah.edu.pk
Umar Abdullah	33073	BSCY	0348-8568636	33073@students.riphah.edu.pk

Mr. Osama Raza
(Senior Lecturer)

Mr. Awais Nawaz
(Teaching Fellow)

NeuroWall

Change Record

Author(s)	Version	Date	Notes	Supervisor's Signature
Muhammad Ubaid Ullah, Hamza Gulzar, Umar Abdullah	1.0	28/08/2024	Original Draft	
Muhammad Ubaid Ullah, Hamza Gulzar, Umar Abdullah	1.2	11/09/2024	Changes Based on Feedback From Supervisor	
Muhammad Ubaid Ullah, Hamza Gulzar, Umar Abdullah	2.0	25/09/2024	Changes Based on Feedback From Faculty	
Muhammad Ubaid Ullah, Hamza Gulzar, Umar Abdullah	2.1	01/10/2024	Changes Based on Feedback From Supervisor	

Project Proposal

Project Title: NeuroWall.

Introduction and Background:

With the rise of more advanced cyberattacks, it's become clear that better security solutions are needed. Traditional firewalls, which use fixed rules, often can't detect or stop the latest threats. Recent events like ransomware attacks and large data breaches have shown that these systems aren't keeping up with how attacks are changing.

This project aims to solve these problems by creating a firewall that uses artificial intelligence (AI) to automatically decide whether to block or allow network traffic. Instead of following set rules, the AI will make decisions based on patterns it learns from network logs. This makes the system more flexible and able to adapt to new threats.

The firewall will also connect with Wazuh, a tool for real-time threat monitoring and alerts. In addition, it will use a VPN to ensure all network traffic is encrypted and secure. Together, these features will add extra protection to the system.

Existing Systems/ Survey/ Literature Review:

Current firewalls, like pfSense and other open-source tools, depend on manually set rules to control network traffic. These rules don't change unless updated, which makes it hard to keep up with new threats. Some systems have started using AI for spotting unusual activity and making predictions, but they still rely on these fixed rules. The lack of flexibility in these setups has created a need for a fully AI-based firewall, where the system makes its own decisions by constantly learning from network traffic.

Wazuh is a popular platform for security monitoring, giving real-time alerts and helping with compliance, but it mainly depends on traditional firewall logs. This project will close the gap by allowing the AI to manage traffic on its own, without needing any preset rules. Also, by adding a VPN, we will ensure that communication is encrypted, keeping sensitive data safe from spying while still letting the AI check for harmful behavior.

Problem Statement:

Traditional firewalls, which rely on preset rules to manage traffic, struggle to keep up with fast-changing cyber threats. These systems often fail to detect new attack methods and need manual updates, leaving them open to attacks in a constantly changing threat environment. They also can't react quickly to threats without a lot of human input. As cyberattacks get more advanced, these rule-based firewalls are becoming less effective, as they aren't flexible enough to handle unknown threats and need constant updating.

There is a clear need for a firewall that can automatically manage network traffic while using a VPN to keep the traffic secure. In addition, by integrating with Wazuh for real-time monitoring and alerts, the system can respond faster to possible threats.

Objectives:

- Build a firewall that uses AI to automatically block or allow network traffic based on its own decisions.

- Train an AI model with log data to spot harmful traffic and adjust to new patterns as they appear.
- Review the AI's decisions to make sure it's accurate in blocking or allowing traffic, reducing false alarms.
- Connect the firewall with Wazuh for real-time monitoring, alerts, and log analysis.
- Add a VPN to secure traffic with encryption, allowing the AI to detect harmful activities even in encrypted channels.

Proposed Solution:

The solution is to create a custom firewall that controls network traffic using only AI-driven decisions. The AI will be trained on past firewall logs to learn how to tell the difference between harmful and safe traffic. The firewall will work with Wazuh for managing logs and sending real-time alerts, so administrators are notified right away if any suspicious activity is found. A VPN will also be added to ensure encrypted data is safely sent, while the AI continues to check for threats within the VPN. By not relying on preset rules, the system can adapt to new threats without needing constant updates.

Methodology:

The AI model will be built using machine learning in Python and trained on large datasets of firewall logs. The firewall will be connected to Wazuh for real-time monitoring and alerting, ensuring any detected threat triggers an instant response. The VPN will use existing protocols to secure traffic while allowing the AI to analyze encrypted traffic for possible threats. This approach balances strong security with flexible threat detection by combining AI and VPN security. Testing will be done in simulated networks to ensure everything works before full deployment.

Implementation Plan:

- **Phase 1**: Train the AI model using real-world firewall log data to recognize different types of traffic.
- **Phase 2**: Build the AI-driven firewall and add the trained model to control traffic decisions.
- **Phase 3**: Test the firewall’s performance by simulating network traffic, including encrypted VPN traffic.
- **Phase 4**: Integrate Wazuh for real-time alerts and set up the VPN for secure communication.
- **Phase 5**: Conduct final testing, optimize performance, and complete project documentation.

Evaluation Plan:

The firewall will be tested for its ability to block harmful traffic, handle VPN traffic, and provide accurate real-time alerts through Wazuh. Evaluation will focus on how well it detects both threats, how accurately it distinguishes between safe and harmful traffic, and

how adaptable it is to new threat patterns. The AI's learning progress will also be monitored to ensure it continues improving as it processes new network data.

Project Scope/ Expected Outcomes:

The project aims to deliver a fully functional AI-driven firewall that can automatically manage network traffic without the need for preset rules. Key outcomes include:

- A trained AI model capable of identifying malicious and safe network traffic.
- A firewall system powered by this AI model, which can make traffic control decisions on its own.
- Full integration of the firewall with a VPN for secure, encrypted communication.
- Integration with Wazuh for real-time monitoring, alerting, and log analysis.
- A complete, tested system that combines AI, VPN encryption, and Wazuh to provide a strong, adaptable security solution.

Conclusion and Future Work:

- This project provides an innovative solution to the problem of static, rule-based firewalls by replacing them with a fully AI-driven approach. The integration of VPNs ensures that even encrypted traffic is secured, while Wazuh adds real-time alerting capabilities. Future work could involve further refinement of the AI model to improve its accuracy in detecting unknown threats, as well as expanding its capability to manage larger-scale network environments or cloud-based infrastructures and develop a system that gets better over time with continuous learning, offering stronger protection against threats.

References:

1. Hasan, M. and Malik, T., 2024, June. AI-Enhanced VPN Security Framework: Integrating Open-Source Threat Intelligence and Machine Learning to Secure Digital Networks. In *European Conference on Cyber Warfare and Security* (Vol. 23, No. 1, pp. 760-768).
2. Zajeganović, M., 2023. pfSense Router and Firewall Software. In Sinteza 2023-International Scientific Conference on Information Technology, Computer Science, and Data Science (pp. 132-137). Singidunum University.
3. Sholihan, Alhu & Mukti, Aan & Suryayusra, Suryayusra & Dasmen, Rahmat. (2023). Implementation of Network Security and Anticipating Attackers Using pfSense Firewall. CESS (Journal of Computer Engineering, System and Science). 8. 175. 10.24114/cess.v8i1.42377.
4. Wang, Z., 2021, September. Research on feature and architecture design of ai firewall. In *2021 5th Annual International Conference on Data Science and Business Analytics (ICDSBA)* (pp. 75-78). IEEE.
5. Wang, Z. and Deng, Q., 2023, October. Research on the Application and Testing Method of AI Firewalls in Network Attack Detection. In *2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)* (pp. 753-757). IEEE.

Work Break down structure

WBS #	WBS Deliverable	Activity # Description	Responsible Team Member(s)
1.0	AI Model Development	Developing and training the AI model for traffic identification.	M.Ubaid Ullah, Umar Abdullah
1.1	Dataset combination and Preprocessing	Combing the datasets mentioned and then preprocessing them	M.Ubaid Ullah, Umar Abdullah
1.2	Model Training	Training the AI model to recognize malicious vs safe traffic.	M.Ubaid Ullah, Umar Abdullah
1.3	Model Evaluation	Testing and fine-tuning the AI model for accuracy.	M.Ubaid Ullah, Umar Abdullah
2.0	Firewall Development	Building the AI-driven firewall system.	Hamza Gulzar, Umar Abdullah
2.1	Design Firewall Architecture	Defining the architecture of the AI-driven firewall system.	Hamza Gulzar, Umar Abdullah
2.2	Develop Custom Firewall	Developing the firewall system based on the AI model's decisions.	Hamza Gulzar, Umar Abdullah
3.0	VPN & Encryption Integration	Integrating VPN for secure communication.	M.Ubaid Ullah, Hamza Gulzar
3.1	VPN Setup	Setting up VPN with encryption to secure traffic.	M.Ubaid Ullah, Hamza Gulzar

3.2	Integrate VPN with Firewall	Connecting VPN with the AI-driven firewall for encrypted traffic analysis.	M.Ubaid Ullah, Hamza Gulzar
4.0	Wazuh Integration	Integrating Wazuh for real-time monitoring and alerts.	Hamza Gulzar, Umar Abdullah
4.1	Wazuh Configuration	Setting up Wazuh for real-time log analysis and alerts.	Hamza Gulzar, Umar Abdullah
5.1	Wazuh & Firewall Integration	Ensuring smooth interaction between Wazuh and the firewall for alerting on malicious traffic.	Hamza Gulzar, Umar Abdullah
6.1	Testing and Validation	Testing and validating the entire system in a controlled environment.	Entire Team
6.2	Simulate Traffic Scenarios	Creating network traffic scenarios to test firewall performance (including VPN traffic).	M.Ubaid Ullah, Hamza Gulzar
6.3	Validate AI Decision Accuracy	Reviewing AI-driven traffic decisions and improving the model as necessary.	M.Ubaid Ullah, Umar Abdullah
6.4	Full System Testing	Testing the entire system (AI firewall, VPN, Wazuh) for performance and reliability.	Entire Team
7.0	Final Optimization & Documentation	Finalizing optimizations and documenting the project for future use and deployment.	Entire Team

7.1	Performance Optimization	Tuning the system for optimal performance based on test results.	M.Ubaid Ullah, Umar Abdullah
7.2	System Documentation	Preparing detailed documentation for the firewall, VPN, and Wazuh integration.	M.Ubaid Ullah, Hamza Gulzar

List of Faculty Proposed Changes

Project Title: NeuroWall

Supervisor's Signature:

Proposed Change	Proposed By	Supervisor's Decision
Clearly Specify your project Scope. What modifications or customizations will be made to pfSense and Wazuh for AI enhancement? Will any specific modules or plugins be developed for this purpose? Will pfSense act as the main traffic filter or will Wazuh also handle certain filtering tasks? Besides, how will two different data sets merge in your project.	Dr. Javed Iqbal	All the highlighted questions have been ~~[illegible]~~ solved in the revised scope.
Clearly mention the technical defects. Research on Technical aspect.	Mr. Mueed Mirza	under consideration
Revise Contribution, data extraction and merging information collection, scope enhancement required.	Mr. Yawar Abbas	under consideration
1. Develop your own Firewall if possible. 2. Look carefully the Wazuh's integration.	Mr. Hammayun	~~1~~ suggestions incorporated

Approval

Project Supervisor

Comments Approved

Name: Muhammad Osama Raza

Date: 2-10-2024 **Signature:**

Project Coordinator

Comments

Name:

Date: **Signature:**