SmartGuard : A Machine Learning Based Classification Framework for Automated DoS/DDoS Defence in Next Generation Firewall Systems

Department of Computer Science and Engineering
PES University, EC Campus, Bangalore, 560100

PROBLEM STATEMENT

Modern firewalls struggle to detect and mitigate real-time DDoS attacks due to high packet rates and evolving traffic patterns. This project aims to build an AI-driven firewall system that captures, classifies, and filters network traffic using ML-based anomaly detection for accurate, low-latency DDoS prevention.

DOMAIN

Cybersecurity and ML Applications

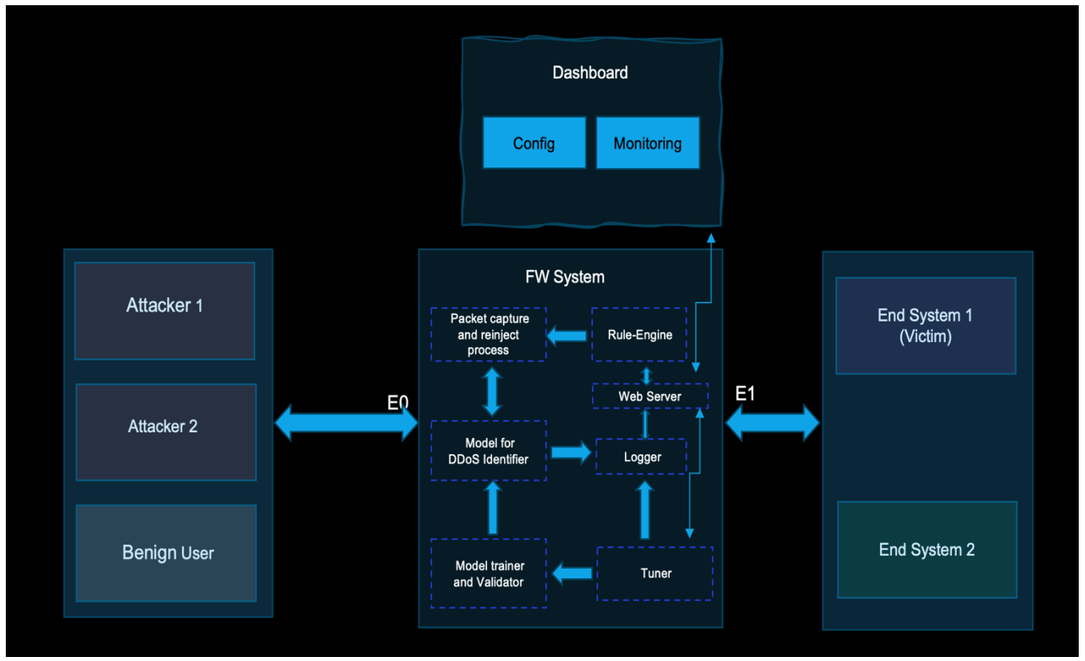
BACKGROUND

Modern networks are increasingly targeted by high-volume and adaptive DDoS attacks that exploit protocol weaknesses and dynamic traffic patterns. Traditional firewalls rely on static, rule-based filtering, which struggles to detect fast-evolving threats, spoofed traffic, and abnormal flow behaviour in real time. As a result, security systems are shifting toward intelligent, ML-driven approaches that can learn normal network behaviour and identify anomalies proactively. This project builds such an approach by combining real-time packet capture, feature extraction, and ML-based classification to create an adaptive, AI-enhanced firewalling system.

PROJECT DESCRIPTION

This project implements an AI-driven firewall system that performs real-time DDoS detection and adaptive traffic control using Scapy for packet capture and processing. Incoming packets are captured, parsed, and converted into flow-level features, which are then classified using a Machine Learning anomaly-detection model. Based on the ML score, the system automatically decides whether to allow, drop, log, or rate-limit the traffic. By integrating Scapy-based packet handling, feature extraction, ML inference, and automated actions, the system provides an intelligent, self-learning defence mechanism against modern high-speed network attacks.

SYSTEM ARCHITECTURE



PROJECT OUTCOME

The project resulted in a fully operational AI-enhanced firewall capable of detecting and mitigating DDoS attacks in real time using Scapy for packet capture and an ML anomaly-detection model for traffic classification. The system successfully integrates live packet processing, feature extraction, model inference, and automated traffic actions—including allowing, dropping, rate-limiting, and logging—based on threat scores. It demonstrates improved responsiveness and accuracy over traditional static firewalls, and provides a complete end-to-end solution with validated performance, scripts, documentation, and reproducible results for future extension.

MENTOR

Kundhavai K R
Assistant Professor

TEAM ID : 152 TEAM MEMBERS

PES2UG22CS418
Pullagura Santosha

PES2UG22CS373
Nitin Pandita

PES2UG22CS055
Aman Kakwani

PES2UG23CS820
Santhosh A

RESULTS AND DISCUSSION

The system successfully detected ICMP, UDP, and TCP SYN flood attacks generated by the attacker scripts. Real-time indicators identified high packet rates, spoofed IPs, large payloads, and unique-port spikes. Firewall actions—None, Drop, and Rate-Limit—were correctly enforced, with dropped-packet counts verified through iptables and logged in JSON. The dashboard reflected live traffic statistics and policy changes accurately. Isolation Forest decision-function histograms for all three attacks showed clear anomaly separation, confirming effective feature extraction and model tuning. Overall, the AI-based firewall provided reliable, adaptive detection and response to multi-protocol DDoS attacks.

CONCLUSION AND FUTURE WORK

The project trained AI models on all key DDoS attack patterns—twelve in total—spanning TCP, UDP, and ICMP. The model was exposed to around 70% varied traffic, covering different packet lengths and rates, and deployed within a Docker-based setup to ensure maximum accuracy under controlled yet realistic traffic conditions. By simulating every attack type, the system successfully visualized traffic behavior on the dashboard and demonstrated all three firewall actions: detection, drop, and rate-limit. Future work can expand the engine to include additional DDoS categories and extend the framework to train models for detecting various malware and virus patterns.

REFERENCES

[1] M. Govindaraj et al., “IntelliSecure AI-Powered Intrusion Detection Framework,” *Proc. 7th Int. Conf. Inventive Computation Technologies (ICICT)*, IEEE, 2024, pp. 365–367.
[2] S. Ahmadi, “Next Generation AI-Based Firewalls: A Comparative Study,” *Int. J. Comput. (IJC)*, vol. 49, no. 1, 2023, pp. 245–262.
[3] K. Dietz et al., “The Missing Link in Network Intrusion Detection: Taking AI/ML Research Efforts to Users,” *IEEE Access*, vol. 12, 2024, pp. 79815–79822.
[4] M. S. Akhtar and T. Feng, “An Overview of the Applications of Artificial Intelligence in Cybersecurity,” *EAI Endorsed Trans. Creative Technol.*, vol. 8, no. 29, 2021.
[5] S. Anbusiranjeevi and J. B. S. Loret, “AI-Based Detection of DDoS Attack by Using Machine Learning,” *Int. J. Res. Anal. Rev.*, vol. 10, no. 2, 2023, pp. 938–941.
[6] N. Berbiche and J. El Alami, “For Robust DDoS Attack Detection by IDS,” *Ingénierie des Systèmes d’Information (ISI)*, vol. 29, no. 4, 2024, pp. 595–606.
[7] J. Ioannidis and S. M. Bellovin, “Implementing Pushback: Router-Based Defense Against DDoS Attacks,” *Proc. NDSS*, San Diego, USA, 2002.