FireGuardCLI – Advanced Firewall Simulation Tool

**Student Name** :Nimmala Madhuri

**Roll Number** :160123737077

**Course**: Cyber Security

**Class**: IT2

**Gitlink:** <https://github.com/nimmalamadhuri467/FireGuardCLI.git>

# 1. Abstract

FireGuardCLI is a command-line-based firewall simulator designed to demonstrate packet filtering, rule management, and network security concepts. It allows simulation of individual or bulk traffic, supports rule priorities, rate limiting, GeoIP filtering, real-time logging, and a statistics dashboard. This project addresses gaps in existing research, such as lack of interactive CLI testing, real-time analytics, and exportable reports. The tool is suitable for both learning and professional testing of firewall configurations.

# 2. Introduction

Firewalls are essential for network security, controlling traffic based on pre-defined rules. Traditional firewall simulators often lack interactivity, logging, or advanced features. FireGuardCLI aims to create a user-friendly, feature-rich simulation environment to help users understand firewall concepts and test realistic network scenarios.

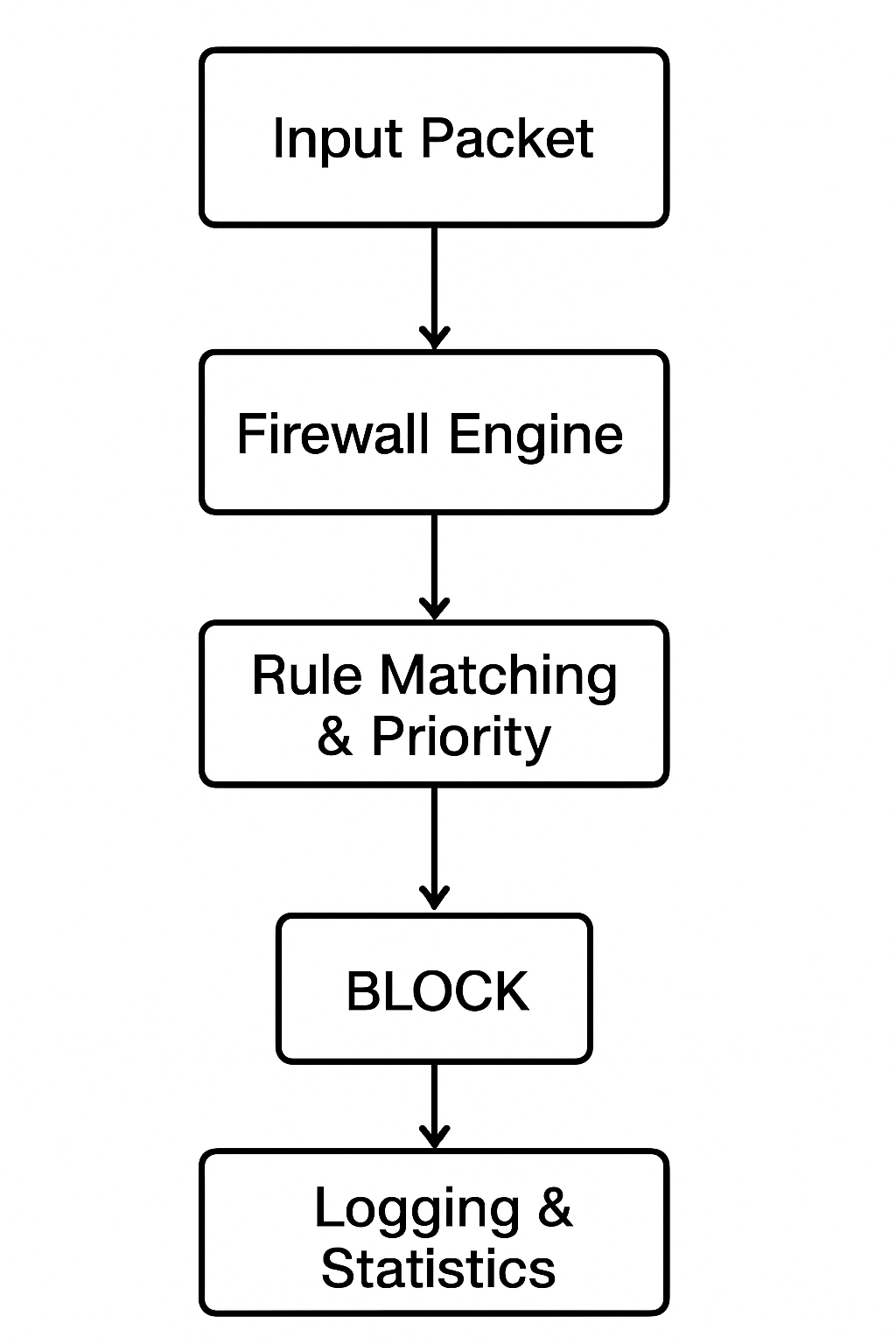
# 3. Literature Review / Paper Summary

- Objective: Basic firewall simulation using rule-based packet filtering.  
- Features: Packet simulation, allow/block rules, basic logging.  
- Gaps:  
 1. No interactive CLI testing  
 2. No GeoIP filtering  
 3. Limited or no real-time logging or statistics  
 4. No bulk packet processing or exportable reports  
  
FireGuardCLI addresses these gaps with advanced features and interactive testing.

# 4. Methodology

## 4.1 Project Overview

FireGuardCLI applies rules to simulated packets and logs decisions. Supports interactive CLI and batch processing.  
 **Architecture Diagram** :



## 4.2 Tools & Technologies

- Language: Python 3.7+  
- Libraries: argparse, JSON, rich, logging, sqlite3, geoip2 (optional)  
- Testing: unittest, pytest

## 4.3 Implementation Details

 simulate <ip> <port> <protocol> – Test a packet against firewall rules

 add-rule – Add a new rule through guided setup

 block <ip> – Quickly block traffic from a specific IP

 allow <ip> – Quickly allow traffic from a specific IP

 delete <rule\_id> – Delete a rule by its ID

 list-rules – Show all rules (optional filters available)

 search <query> – Search rules by IP or description

 stats – Show firewall statistics

 logs – View recent firewall logs

 export <filename> – Export current rules to a file

 reset – Reset all rules and logs (dangerous!)

 clear – Clear the CLI screen

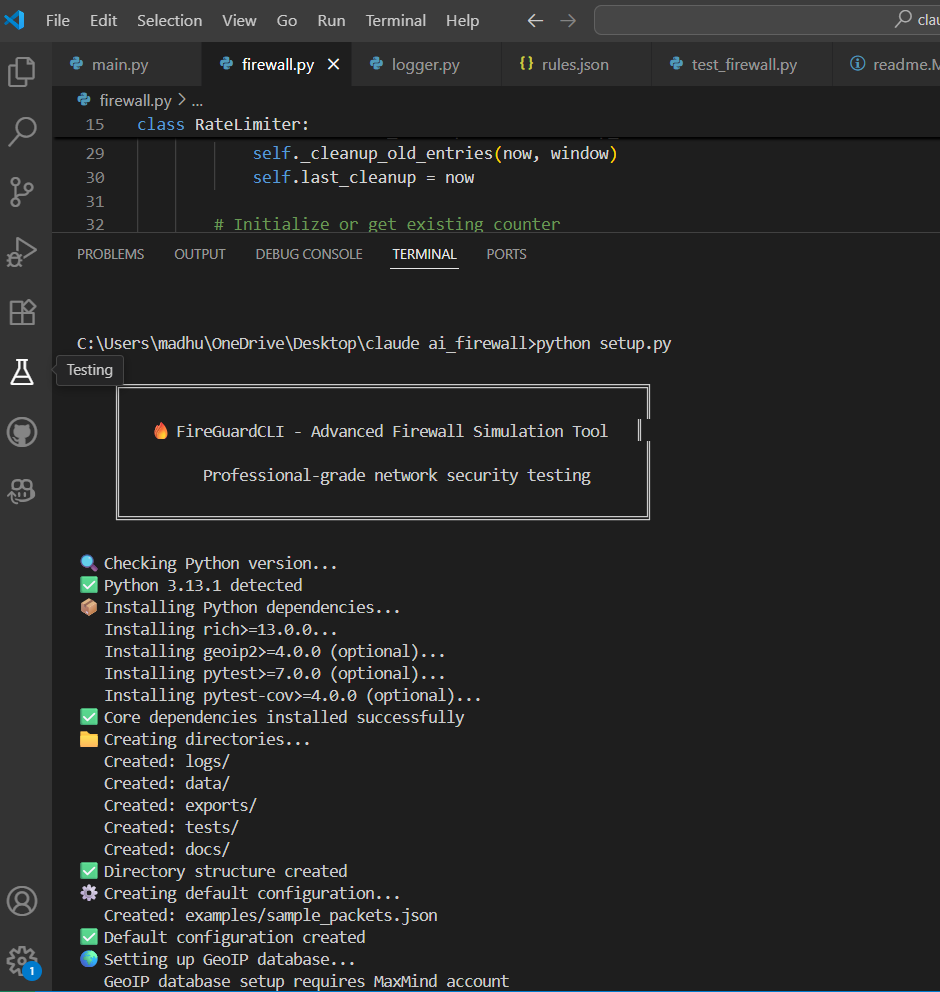
 help – Display help information

 quit – Exit interactive mode

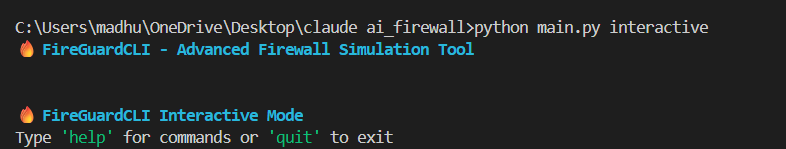
# 5. Results

|  |  |  |
| --- | --- | --- |
| Test Scenario | Expected Outcome | Result |
| Single packet simulation | Correct ALLOW/BLOCK | ✅ |
| Bulk packet simulation (100 packets) | Accurate statistics | ✅ |
| Add/Delete Rule | Rule reflected | ✅ |
| GeoIP Block | Traffic blocked by country | ✅ |
| Statistics Dashboard | Correct counts & rates | ✅ |

**1.Screenshots of Results:**

****

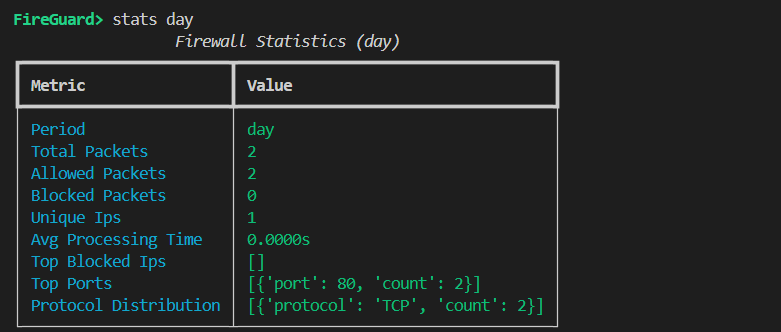
**2. Interactive CLI Mode**

****

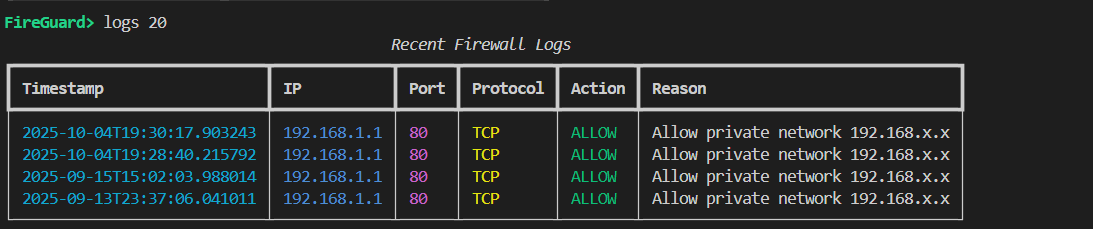
**3.** **Packet Simulation**

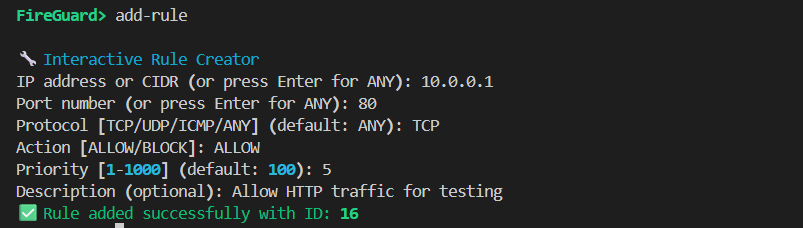
****

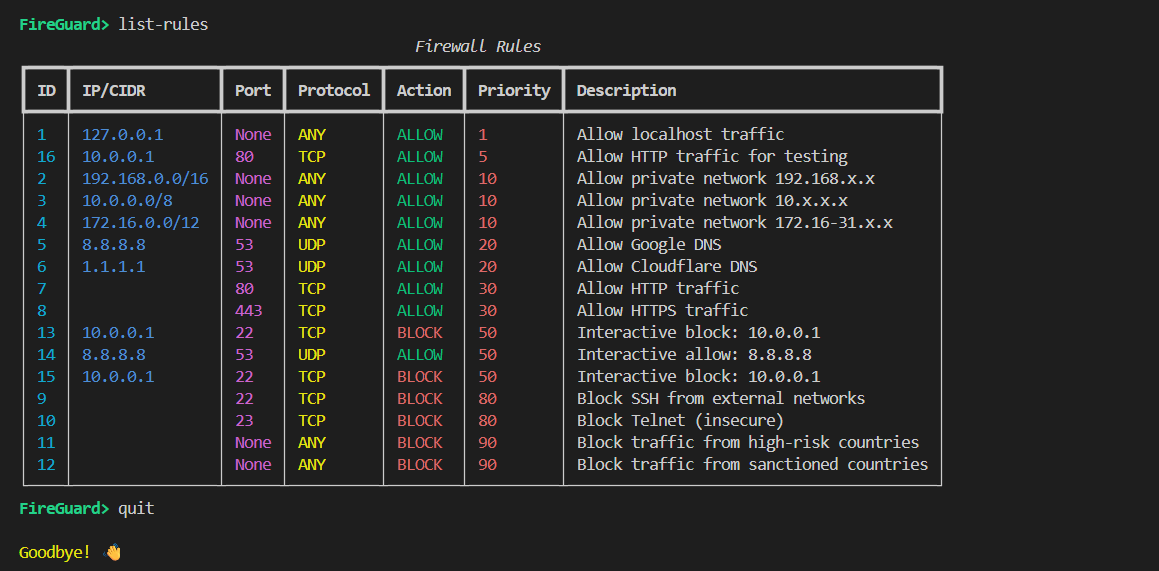
**4.** **Statistics**

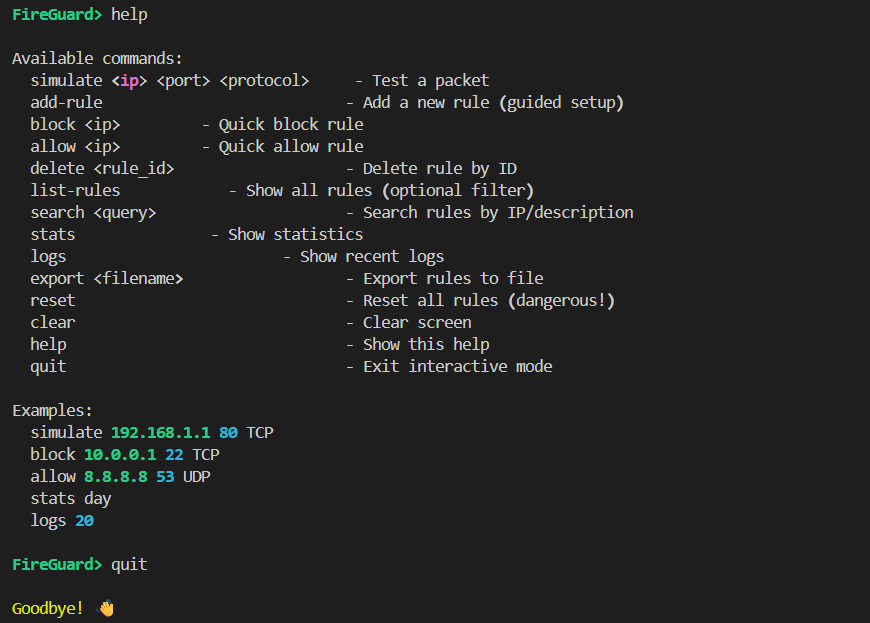
****

**5. Logging**

****

**6. Rule Management**

**7.List Rules: **

**8.Help and quit **

# 6. Conclusion

FireGuardCLI successfully simulates firewall behavior and addresses limitations in prior research. It provides interactive testing, advanced rule management, real-time logging, statistics dashboards, and optional GeoIP filtering—making it both educational and practical.

# 7. References

* [Research Paper Citation in IEEE/APA <https://www.ijcert.org/index.php/ijcert/article/view/1088/913>]