Personal Firewall Project – Summary

---

1. Abstract

A cross-platform Python firewall app was developed using Scapy for packet analysis, Tkinter for GUI, and system-level integrations (iptables, WinAPI). It offers features like port scan and flood detection, audit logging, and dual UI (GUI + CLI) for personal or educational use.

2. Purpose

Existing firewalls are often expensive or inflexible. This project delivers real-time monitoring, rule-based filtering, and threat detection in a simple and customizable form.

3. Key Technologies

Layer	Tools
Language	Python 3.7+
Packet Analysis	Scapy 2.4.5
UI	Tkinter, CLI (argparse)
Metrics	psutil 5.8
System Access	iptables (Linux), WinAPI

4. Core Components

- **PacketSniffer**: Multi-threaded capture (TCP/UDP/ICMP)
- **RuleManager**: JSON rules (IP, port, CIDR)
- **ThreatDetector**: Scan/flood detection
- **LogManager**: Text + JSON logs
- **UI Layer**: Tabbed GUI, mirrored CLI

5. Development Highlights

- Modular design, threading, and live analysis
- GUI/CLI parity for accessibility
- Platform integration with privilege checks
- Demo mode for testing without admin rights

6. Features

- Real-time traffic stats and rule editor

- Intelligent filtering and anomaly alerts
- Exportable, tamper-evident logs
- Adjustable performance parameters

7. Performance & Platform

- Handles ~10K packets/sec on 4-core CPU
- Runs on Windows 10+, Ubuntu 18.04+, CentOS 7+
- Compact footprint, PyInstaller bundle

8. Security

Feature	Method
Filtering	Stateless + stateful
DoS Defense	Rate-limiting, flood control
User Privilege	Elevated only for system rules
Config Integrity	SHA-256 + auto backup

9. Limitations & Future Plans

- SSL inspection in dev
- Threat feed integration (v2)
- macOS support pending
- Planned mobile alert app

10. Conclusion

This Python-based firewall proves that serious network protection can be user-friendly, customizable, and open source. It's modular, performant, and ideal for learning or light enterprise use.

11. Snapshot (v1.0)

- ~2,500 LOC · 13 modules · 15+ features
- 10,000+ word documentation
- Released June 2025 · GPL-3.0

Prepared by: Tanim Naha