# Personal Firewall using Python

**Introduction**
Firewalls are essential in protecting hosts from unwanted network traffic. This lightweight project implements a personal firewall in Python that inspects packets in real-time, applies user-defined rules (IP/port), logs activity, and optionally provides a simple GUI for monitoring.

**Abstract**
The goal of this project is to demonstrate basic packet-filtering and monitoring using Python and Scapy. The firewall captures packets from a specified network interface, compares packet attributes against a JSON-based ruleset (blocked IPs and ports), logs allowed/blocked events, and can present live stats via a Tkinter GUI.

**Tools Used**
• Python 3 (language)
• Scapy (packet sniffing and parsing)
• Tkinter (optional GUI)
• rules.json (user-editable rules file)
• Log file: firewall_log.txt (for auditing)

**Steps Involved in Building the Project**
1. Environment setup: install Python 3, pip and Scapy. Ensure the script runs with root/administrative privileges (packet sniffing requires elevated rights).
2. Packet capture: use Scapy's sniff() function bound to a network interface to receive packets in real time.
3. Packet parsing: examine packet layers (Ether/IP/TCP/UDP) and extract source/destination IP and ports.
4. Rule evaluation: load blocked_ips and blocked_ports from rules.json, then match each packet against the ruleset.
5. Action & logging: if a packet matches a block rule, log a BLOCKED entry (timestamp, src→dst, proto, reason); otherwise log ALLOWED.
6. Optional GUI: implement a Tkinter window to display live logs, counters for blocked/allowed packets, and inputs to add rules at runtime.
7. (Optional) System-level enforcement: integrate with iptables (Linux) for kernel-level blocking if required for stronger enforcement.

**How to run (example)**
1. Install dependencies: *sudo apt update && sudo apt install -y python3 python3-pip python3-tk* then *python3 -m pip install --user scapy*.
2. Edit rules.json to include IPs/ports to block.
3. Run with elevated privileges: *sudo python3 firewall.py --iface eth0* (replace eth0 with your interface).

**Conclusion**
This project provides a compact, educational personal firewall demonstrating packet inspection, rule-based filtering, and logging using Python and Scapy. It is suitable for learning network security concepts and can be extended with features such as protocol-specific rules, dynamic rule updates, or kernel-level blocking for production use.

*Reference:* Project repository: https://github.com/JAGANNADH18/Personal-Firewall-using-Python