Linux Exam Firewall – Technical Design Specification (Draft)

I. Executive Summary & Problem Scope

The Problem

During in-school quizzes and exams, students often access unauthorized online resources such as AI tools (e.g., ChatGPT), gaming websites (e.g., chess.com), and streaming services (e.g., Netflix). Traditional device-level controls are difficult to enforce, easy to bypass, and inconsistent across operating systems. This creates academic integrity concerns and increases the administrative burden on instructors and IT staff.

The Solution

This project implements a **Linux-based network firewall** that centrally controls and restricts internet access during exams. The firewall sits between student devices and the internet, filtering traffic using DNS-based blocking and firewall rules. Because the control happens at the network level, no software is required on student devices, and restrictions apply equally across Windows, macOS, and Linux systems.

Target Users

- **Primary Users:** School IT administrators and instructors
- **Secondary Users:** Students taking quizzes or exams on school-provided or personal laptops

---

II. Technical Requirements

Functional Requirements

- The system must route all student network traffic through a dedicated Linux firewall.
- The system must block access to:
    - AI tools (e.g., ChatGPT, OpenAI domains)
    - Online games (e.g., chess.com)
    - Streaming platforms (e.g., Netflix)
- The system must prevent users from bypassing restrictions by changing DNS settings.

- The system must allow normal academic and educational websites to function normally.
- The system must support Windows, macOS, and Linux client devices without client-side software installation.

Non-Functional Requirements

- The firewall must be stable and capable of running continuously during school hours.
- DNS responses should resolve in under 100 ms to avoid noticeable latency.
- Firewall rules must persist after reboot.
- The system should be simple enough to be maintained by a high school–level IT team with documentation.

III. System Architecture & Logic

System Architecture Overview

The system uses a **dual-homed Linux server** with two Ethernet interfaces:

- **WAN Interface:** Connected to the internet (router/modem)
- **LAN Interface:** Connected to student devices via a switch or Wi-Fi access point

All student traffic must pass through the Linux server, allowing centralized enforcement of network rules.

None

```
Internet
   |
[ Router / Modem ]
   |
[ Linux Firewall Server ]
   |   (LAN Interface)
[ Switch / Wi-Fi Access Point ]
   |
[ Student Devices ]
```

Logic Flow (High-Level)

1. A student device sends a request to access a website.
2. Traffic is routed to the Linux firewall via the LAN interface.

3. DNS requests are handled by dnsmasq on the firewall.
4. If the domain is on the block list, dnsmasq returns `0.0.0.0`.
5. If the domain is allowed, traffic is forwarded to the internet via the WAN interface.
6. Firewall rules prevent DNS bypass attempts and block known VPN ports.

IV. Data Schema & Tech Stack

Tech Stack

Component	Technology	Justification
Operating System	Ubuntu Server 22.04 LTS	Stable, long-term support, widely used in industry
Firewall	iptables	Low-level, reliable Linux firewall control
DNS Filtering	dnsmasq	Lightweight, fast, easy to configure for domain blocking
Persistence	iptables-persistent	Ensures rules survive reboots

The selected stack prioritizes stability, transparency, and ease of maintenance over complexity.

Data Model

This system does not store personal user data. Configuration data includes:

- Blocked domain list (text-based)
- Firewall rules (iptables)
- Network interface configuration

No student-identifiable information is logged or retained in the base implementation.

V. Open Questions & Potential Problems

1. Open Questions (Known Unknowns)

- Should the firewall support a scheduled "Quiz Mode" that automatically enables/disables blocking?
- Is additional VPN detection required beyond common ports (e.g., TLS-based VPNs)?

- Should logging be enabled to record attempted access to blocked sites, and if so, how long should logs be retained?

2. Risk Assessment & Mitigation Table

Potential Problem	Impact	Mitigation Plan
Students attempt DNS bypass	High	Block all outbound DNS except firewall
VPN usage to bypass firewall	High	Block common VPN ports and protocols
Firewall misconfiguration causes internet outage	Medium	Maintain rollback commands and documented recovery steps
Hardware failure of firewall PC	Medium	Use backup hardware or VM image

3. AI Integration & Vetting Appendix

Prompt Log

- "Design a Linux-based firewall to block AI tools, gaming, and streaming websites during school exams."
- "What is a secure and simple way to force DNS-based blocking on Ubuntu Server?"
- "How can a dual-network-interface Linux firewall be explained clearly in a design document?"

My Work and use of ai:

AI was used only to help with design ideas and solving problems, like a senior mentor. The student created, tested, and confirmed all configurations, commands, and design decisions by themselves. The final system shows the student’s own understanding and responsibility for the work.

Google Search, Claude, Gemini, and ChatGPT were used for learning support because Linux is not a fully known language for us. These tools were used only to understand concepts, follow best practices, and find possible mistakes early.

Milestones (Draft)

- Week 1: Linux installation and network interface setup
- Week 2: Firewall and DNS blocking configuration
- Week 3: Testing with Windows, macOS, and Linux devices
- Week 4: Documentation, risk review, and optional feature expansion