Lab Report

Computer Networks Labratory

Submitted to:

Abu Naim Khan

Lecturer

Department of Computer Science and Engineering

North Western University,Khulna

Submitted by:

Md Khan Bahadur Sadi

ID :20231129010

Department of Computer Science and Engineering

North Western University,Khulna

Title

ISP-Level Internet Control and Content Filtering System

Introduction

The internet plays a vital role in modern communication, education, and business. However, unrestricted access can expose users to inappropriate, harmful, or non-productive content. To prevent this, Internet Service Providers (ISPs) implement network-level internet control and content filtering systems.

This system allows ISPs to monitor traffic, block restricted websites, and manage bandwidth usage effectively. By using DNS filtering, proxy servers, and Access Control Lists (ACLs), ISPs can ensure safe and policy-compliant internet access while maintaining efficient network performance.

Required Devices and Tools

Device / Tool	**Purpose**
Router	To control and route internet traffic
Switch	To connect multiple client PCs within the LAN (Local Area Network)
DNS Server	To perform domain-based filtering
Proxy Server / Firewall	For content filtering and traffic monitoring
Meraki Server	**To centralize network management, configuration, and monitoring of Meraki devices (e.g., switches, access points) via the cloud.**

Client PCs	To test browsing and access control
Cisco Packet Tracer / GNS3	For network simulation and configuration
Ethernet Cables	To establish physical or simulated connections

OverView

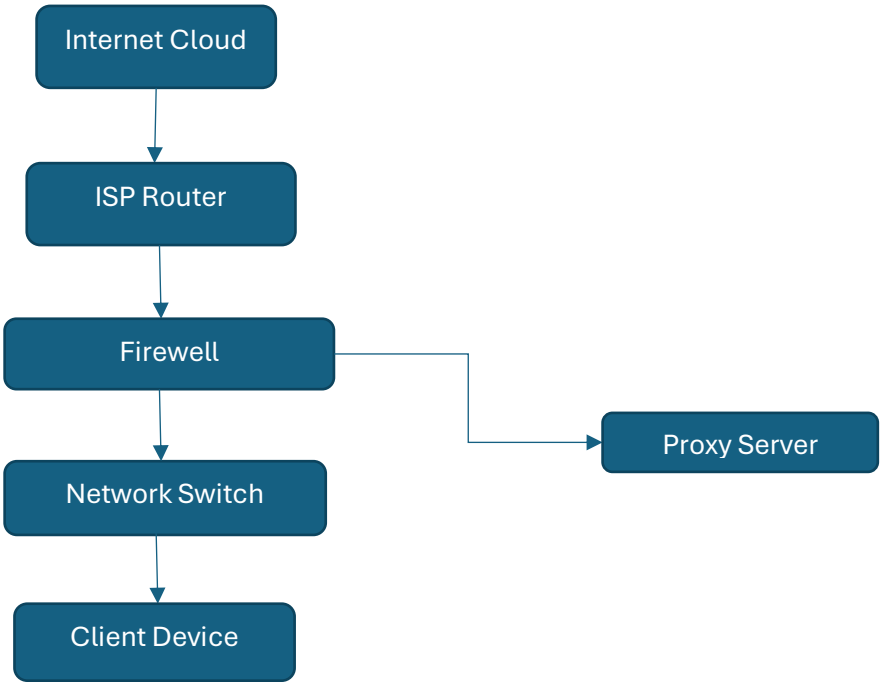

Figure: Basics Diagram of **ISP-Level Internet Control and Content Filtering System**

The **ISP-Level Internet Control and Content Filtering System** is a network security mechanism designed to monitor, manage, and restrict online content at the Internet Service Provider (ISP) level. Instead of relying on user-side tools, this system operates at the core of internet distribution, filtering data before it reaches end users.

In this lab, the system was simulated using **Cisco Packet Tracer** to demonstrate how ISPs can use **routers, firewalls, and access control lists (ACLs)** to block specific websites or categories of content such as adult, gambling, or malicious sites. The project highlights how ISPs can ensure a safer and more controlled internet experience by implementing centralized filtering policies.

Through this experiment, students gained practical knowledge of **network topology design**, **firewall configuration**, and **traffic control techniques**, which are essential for maintaining secure and ethical internet services in modern network environments.

Advantages

- Centralized control for multiple clients.
- Enhanced cybersecurity and user protection.
- Customizable blocking policies.
- Can integrate AI-based content analysis APIs for improved accuracy.

Limitations

- High maintenance and updating required for blocklists.
- May sometimes block harmless sites due to keyword overlap.
- SSL-encrypted (HTTPS) traffic filtering requires deep packet inspection (DPI), which can affect performance.

Future Scope

- Integration with **Machine Learning** to detect harmful content dynamically.
- Real-time updates via **AI-powered filtering APIs** (e.g., Kahf Guard).
- Cloud-based centralized management dashboard for ISPs.
- Adding parental control and time-based restrictions for users.

Conclusion

The ISP-Level Internet Control and Content Filtering System proved to be an efficient and scalable approach to maintaining a safe and controlled digital environment. By

implementing filtering mechanisms directly at the Internet Service Provider (ISP) layer, it becomes possible to restrict access to malicious, inappropriate, or non-compliant web content before it reaches end users. This proactive strategy significantly strengthens **network security**, minimizes exposure to **cyber threats**, and helps ensure **regulatory compliance** with national and organizational internet policies.

Through the practical simulation in **Cisco Packet Tracer**, the system successfully demonstrated how ISPs can utilize **firewalls**, **Access Control Lists (ACLs)**, and **DNS or keyword-based filtering** to monitor and manage internet traffic efficiently. The results confirmed that targeted websites and content types were effectively blocked while legitimate traffic remained uninterrupted, showcasing the balance between control and accessibility.

Overall, this experiment highlights the importance of deploying **centralized filtering at the ISP level** to protect a large number of users simultaneously, reduce the burden on end-user devices, and encourage **responsible and secure internet usage**. Future developments can integrate **AI-driven filtering**, **real-time analytics**, and **cloud-based APIs** to enhance adaptability and precision in content management systems.