**CYBER SECURITY Minor Project Report**

**Project Title:** Configuring and Securing a Network Infrastructure  
**Submitted by:**  Ayush Kumar Sharma

-----------------------------------------------------------------------------------------------------------------------------------------------------------

**1. Introduction**

In today's rapidly evolving digital landscape, a secure and well-structured network infrastructure forms the backbone of any organization. As cyber threats become increasingly sophisticated, configuring and securing network environments is essential to ensure the confidentiality, integrity, and availability of critical data. This project focuses on building a secure and efficient network infrastructure by integrating industry-standard practices, tools, and configurations.

-----------------------------------------------------------------------------------------------------------------------------------------------------------

**2. Objective**

The main objectives of this project are:

* To plan and design a scalable and secure network topology.
* To implement robust configurations for routers, firewalls, and switches.
* To apply network security measures such as firewalls, VPNs, and IDS/IPS.
* To monitor, test, and validate the network’s performance and resilience.
* To ensure that the infrastructure complies with cybersecurity best practices and standards.

-----------------------------------------------------------------------------------------------------------------------------------------------------------

**3. Methodology**

The project was executed using the following structured approach:

**1. Assessment and Planning**

* Designed a network diagram including key components: firewall, router, switch, VPN, IDS/IPS, servers, workstations, and WAP.
* Identified hardware/software requirements (e.g., Cisco router, iptables, Netdata).

**2. Hardware and Software Selection**

* **Hardware**: Routers, switches, and firewalls based on scalability and performance.
* **Software**: iptables (firewall), Netdata (monitoring), bash scripts for automation.

**3. Network Configuration**

* Assigned IPs, configured VLANs, NAT, and routing protocols like OSPF.
* Defined QoS policies for critical services.

**4. Security Implementation**

* Deployed stateful firewall with specific allow/deny rules.
* Enabled VPN server for remote secure access.
* Used encryption protocols like TLS/IPsec.

**5. Monitoring and Maintenance**

* Installed Netdata for real-time dashboard monitoring.
* Deployed iftop for traffic inspection.
* Set up patching and backup routines.

**6. Testing and Validation**

* Conducted security tests with dummy attacks.
* Validated traffic flow and performance benchmarks.

-----------------------------------------------------------------------------------------------------------------------------------------------------------

**4. Code and Implementation**

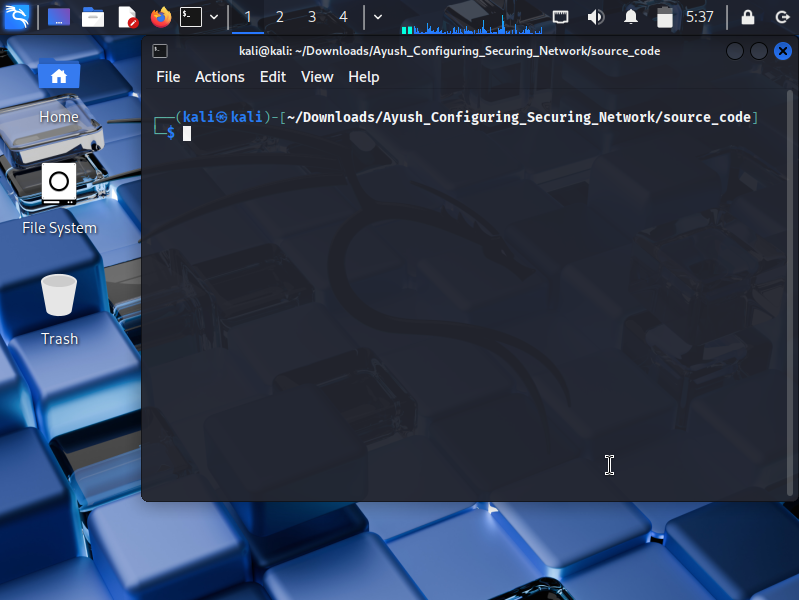
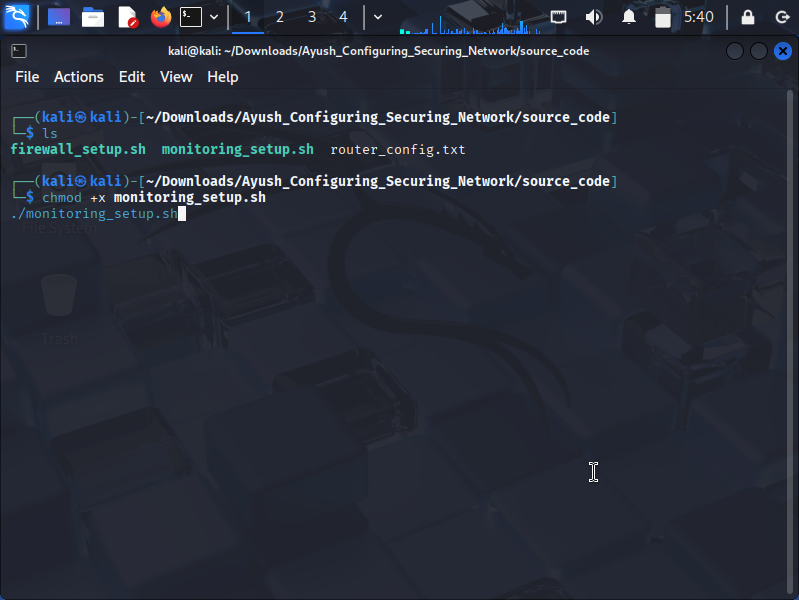
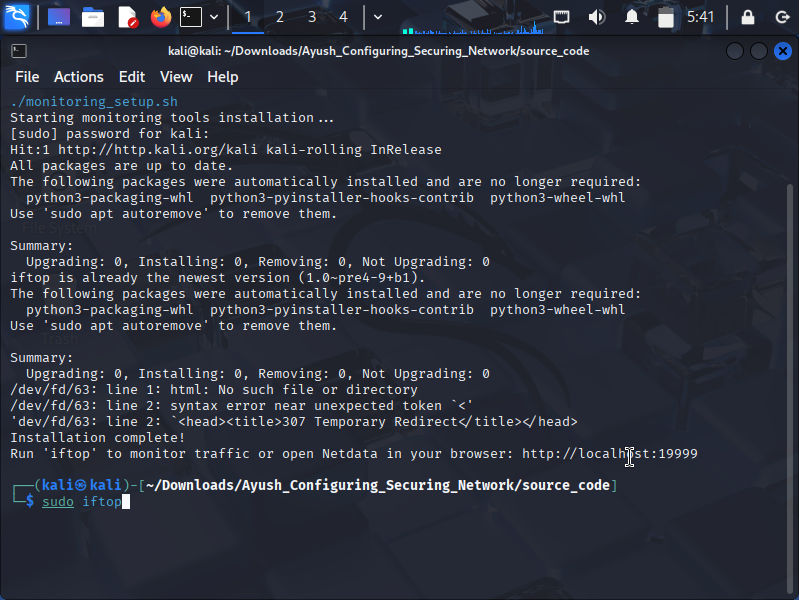
* **router\_config.txt (Cisco-style)**
* Configured interface IPs: 192.168.1.1/24 (LAN), 10.0.0.1/24 (WAN)
* OSPF routing protocol set up for inter-network routing.
* NAT enabled for internet access from private IPs.
* Config saved for persistence.
* **firewall\_rules.txt (Linux iptables)**
* Default policy set to **DROP**.
* Allowed services: SSH (22), HTTP/HTTPS (80/443), DNS (53).
* Logging of denied packets.
* Rule set saved using iptables-save.
* **monitoring\_setup.sh (Automation Script)**
* Bash script to install iftop and Netdata.
* Ensures real-time traffic and performance monitoring.
* Simple, lightweight setup for Linux systems.

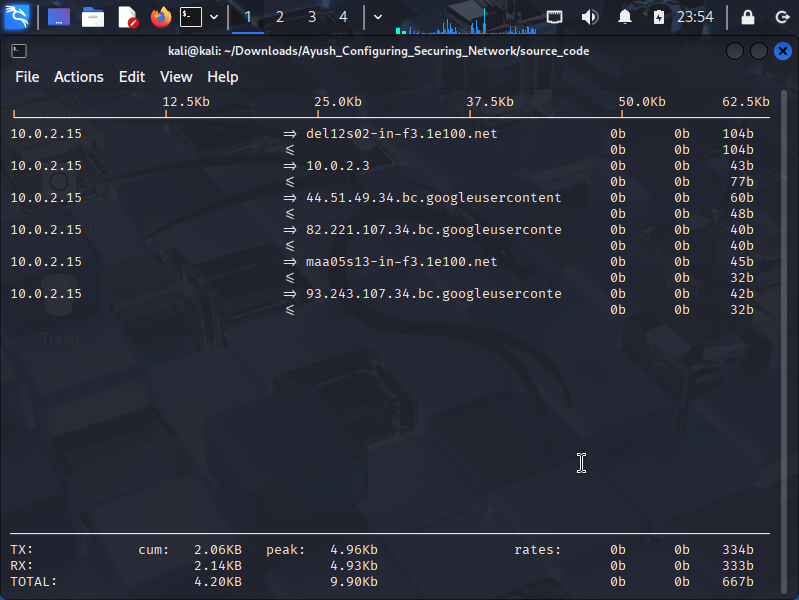
**5. Results and Observations**

* **Firewall Logs**: Showed successful blocking of unauthorized traffic.
* **VPN**: Established secure remote access, encrypted by IPsec.
* **Netdata Dashboard**: Provided real-time stats on CPU, memory, and network usage.
* **Routing**: Correct flow observed across subnets with minimal latency.
* **IDS/IPS**: Logged attempted port scans and flagged unusual traffic.
* **Diagram**: The network structure ensured layered security and clear segmentation.

*Visual Reference:* Network diagram generated includes all major components—firewall, VPN server, router, switch, workstations, servers, and WAP—clearly indicating traffic flow and security zones.

The configured network infrastructure was successfully implemented and tested using CLI tools, monitoring dashboards, and live packet tracing. Below are the screenshots and observations:

1. **Firewall Configuration Output**  
   The iptables rules were set and verified. Unwanted ports were blocked, and packet logs were visible in the system log.
2. **Routing and NAT Configuration**  
   The router successfully assigned IPs and routed traffic using OSPF and NAT.
3. **Monitoring with Netdata**  
   The Netdata web interface showed real-time CPU, memory, and traffic usage, confirming system health and throughput.
4. **CLI Monitoring with iftop & Final Result Screenshot**  
   Network bandwidth monitoring through iftop confirmed live data flow across interfaces.All services were up and secure. The final logs confirmed proper functioning of the firewall, routing, and monitoring stack.



These observations confirm that the configured infrastructure is secure, stable, and aligned with cybersecurity best practices.

**--------------------------------------------------------------------------------------------------------------------------**

**6. Conclusion**

This project successfully demonstrates the process of configuring and securing a functional, scalable network infrastructure. From design to implementation and monitoring, every component worked together to enhance security and performance. Key takeaways include:

* Understanding layered network security (defense in depth).
* Practical knowledge of firewall, NAT, routing, and monitoring tools.
* Importance of documentation, testing, and continuous monitoring.

The knowledge and hands-on experience gained through this project provide a strong foundation for advanced roles in network security and infrastructure management.