PROJECT REPORT
Name Sudhir S Bhat
Title: Network Security Fundamentals

1. Project Overview

In this project, I explored the core **building blocks of network security**, focusing on Firewalls, **Intrusion Detection Systems (IDS)**, and **Intrusion Prevention Systems (IPS)**.
The objective of this project was not to perform hacking or exploitation, but to **understand how organizations defend their networks** from unauthorized access, malicious traffic, and cyber attacks.
This project simulates real-world enterprise network protection concepts that are widely used in **SOC (Security Operations Center)** and **Network Security Engineer** roles.

2. Objective of the Task

The main objectives of this task were
To understand **why network security is critical** in modern organizations
To learn **how firewalls control network traffic**
To study **how IDS and IPS detect and prevent attacks**
To understand the **difference between detection and prevention**
To build **security awareness from a defensive perspective**

3. Introduction to Network Security

Network security focuses on **protecting data, systems, and users** as information travels across networks.

In today's environment

- Employees work remotely
- Cloud and on-premise systems coexist
- Attackers continuously scan networks for weaknesses

Without network security controls, an organization becomes an open target for

- Malware infections
- Data breaches
- Unauthorized access
- Service disruptions

4. Firewalls – The First Line of Defense

What is a Firewall?
A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.
Think of a firewall as a security guard at the network entrance

- It allows trusted traffic
- It blocks suspicious or unauthorized traffic

Types of Firewalls
1. Packet Filtering Firewall

- Examines IP addresses, ports, and protocols
- Fast but limited visibility
- Used in basic network setups

2. Stateful Firewall

- Tracks active connections
- More intelligent than packet filtering
- Common in enterprise networks

3. Application / Next-Generation Firewall (NGFW)

- Inspects application-level traffic
- Can block malware, exploits, and malicious URLs
- Used in modern enterprise environments

Why Firewalls Are Important

- Prevent unauthorized access
- Reduce attack surface
- Enforce network security policies
- Protect internal systems from the internet

5. Intrusion Detection System (IDS)

What is IDS?
An **Intrusion Detection System (IDS)** monitors network or system activity to **detect suspicious behavior or known attack patterns**.
Unlike firewalls

- IDS **does not block traffic**
- IDS **alerts security teams** when something suspicious occurs

Types of IDS

1. Network-Based IDS (NIDS)

- Monitors network traffic
- Detects attacks like port scanning, DoS, malware traffic

2. Host-Based IDS (HIDS)

- Installed on individual systems
- Monitors logs, file changes, and system activity

How IDS Detects Attacks

- **Signature-based detection** (known attack patterns)
- **Anomaly-based detection** (unusual behavior)

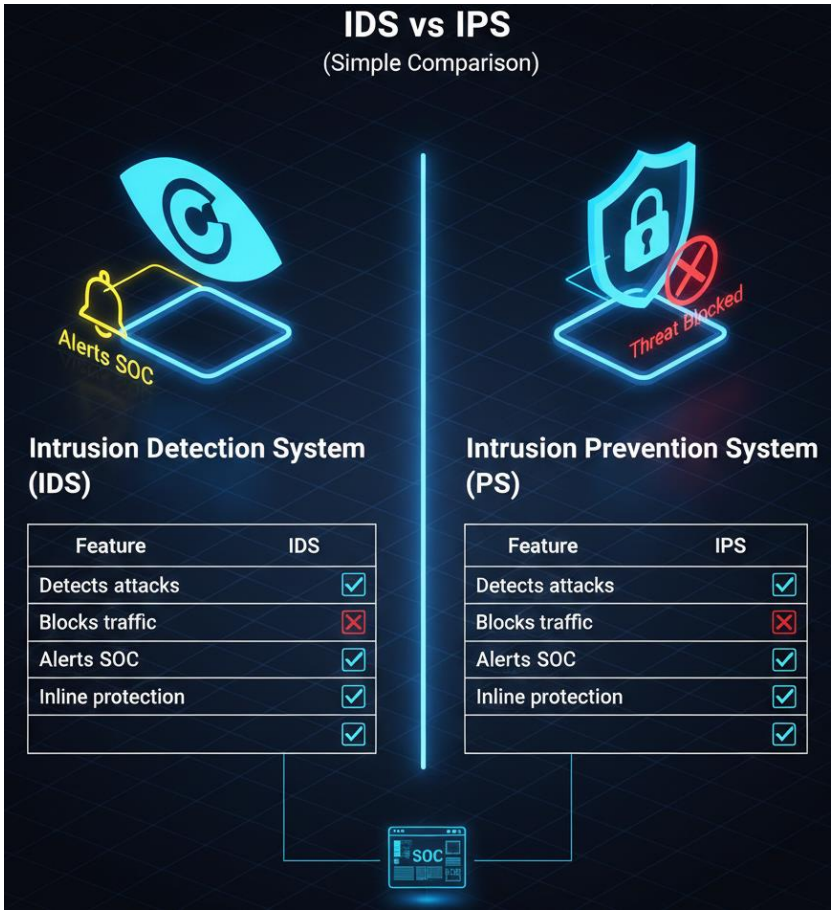
6. Intrusion Prevention System (IPS)

What is IPS?

An **Intrusion Prevention System (IPS)** is similar to IDS but with one major difference

- IPS can automatically block or prevent malicious traffic

IDS vs IPS (Simple Comparison)



Why IPS Is Critical

- Stops attacks in real time
- Reduces incident response time
- Protects against known exploits automatically

7. Real-World Enterprise Scenario

In a real organization

- **Firewall** controls which traffic enters the network
- **IDS** monitors traffic and generates alerts
- **IPS** blocks confirmed malicious activity
- **SOC analysts** investigate alerts and respond to incidents

This layered approach is called Defense in Depth.

8. Security Best Practices Learned

During this project, I learned the importance of

- Proper firewall rule configuration
- Regular rule reviews to avoid misconfigurations
- IDS tuning to reduce false positives
- Continuous monitoring and alert analysis
- Combining tools instead of relying on a single control

9. Outcomes

By completing this task, I achieved the following outcomes:

- Strong understanding of network security fundamentals
- Ability to explain firewalls, IDS, and IPS clearly
- Awareness of SOC monitoring workflows
- Improved confidence for technical awareness
- Hands-on theoretical readiness for real enterprise environments

It aligns well with organizations goal of building industry-ready cybersecurity professionals.

10. Lessons Learned

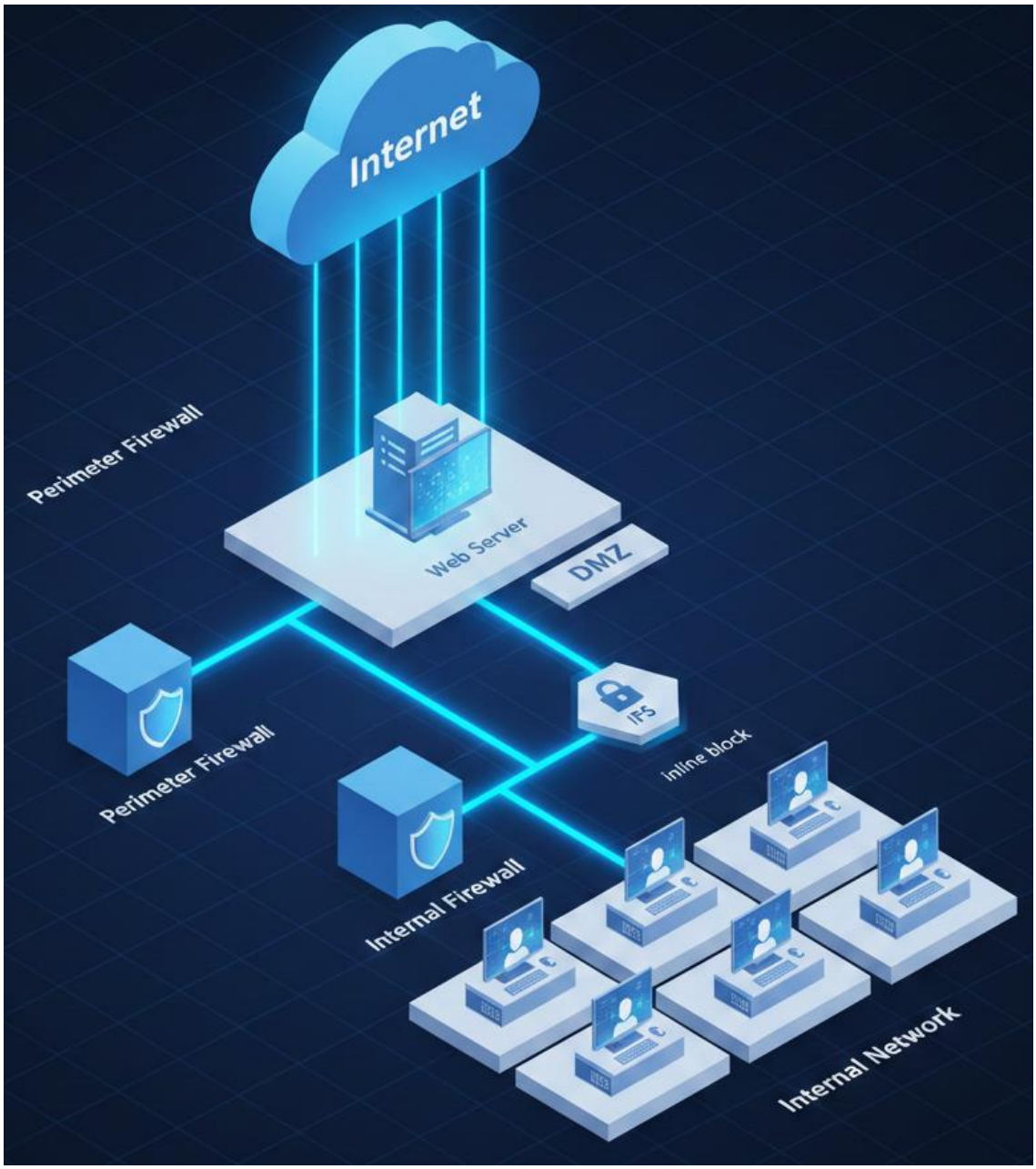
Some key lessons learned from this project

- Prevention is always better than response

- Misconfigured firewalls can be as dangerous as no firewall
- IDS alerts require human analysis
- Security tools must be properly tuned
- Network security is a continuous process, not a one-time setup

11. Diagrams

Enterprise Firewall Architecture



IPS Traffic Flow

Network Security

12.Conclusion

This project helped me build a **strong foundation in network security concepts**. By understanding how firewalls, IDS, and IPS work together, I gained insight into how organizations protect their networks from modern cyber threats.
As a intern, this task prepared me for **SOC L1 roles, network security, and future hands-on labs**, making it a valuable learning experience in my cybersecurity journey.