FIREWALL RULES DOCUMENTATION

1. Introduction

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between trusted and untrusted networks.

2. Objectives

- Protect the network from unauthorized access

- Allow only trusted traffic

- Block malicious and suspicious activities

- Monitor network communication

3. Types of Firewalls

- Network Firewall

- Host-based Firewall

- Hardware Firewall

- Software Firewall

- Cloud Firewall

4. Common Firewall Rules

Rule 1: Allow HTTP Traffic

Port: 80

Action: Allow incoming and outgoing web traffic

Rule 2: Allow HTTPS Traffic

Port: 443

Action: Allow secure web browsing

Rule 3: Allow SSH Access

Port: 22

Action: Allow secure remote login for administrators

Rule 4: Block Telnet

Port: 23

Action: Block insecure remote access

Rule 5: Block FTP (if not required)

Port: 21

Action: Prevent unauthorized file transfer

Rule 6: Deny All Other Traffic

Action: Block all unspecified or suspicious traffic

5. Linux Firewall (UFW) Commands

Enable Firewall: sudo ufw enable

Check Status: sudo ufw status

Allow HTTP: sudo ufw allow 80

Allow HTTPS: sudo ufw allow 443

Allow SSH: sudo ufw allow 22

Block Telnet: sudo ufw deny 23

Disable Firewall: sudo ufw disable

6. Best Practices

- Regularly update firewall rules
- Close unused ports
- Monitor firewall logs
- Use strong authentication
- Enable intrusion detection systems
- Backup firewall configuration

7. Conclusion

Firewall configuration is essential for network security. Proper firewall rules protect systems and networks from cyber threats and unauthorized access.