# Summary of Cybersecurity Firewall Lab

In this lab exercise, I set up a virtual firewall appliance using pfSense within VirtualBox to simulate a network security environment. The main goal was to configure and test firewall rules, enabling secure communication between an internal LAN and the external WAN, and to integrate an Intrusion Detection/Prevention System (IDS/IPS) to monitor network traffic.  
  
Key activities included:  
  
- Downloading and preparing the pfSense ISO image for installation in VirtualBox.  
- Creating and configuring multiple network adapters in VirtualBox to simulate WAN and LAN interfaces.  
- Installing pfSense and performing initial setup via the web interface.  
- Setting firewall rules to allow traffic from LAN to WAN while restricting unwanted access.  
- Configuring and enabling Snort IDS/IPS to detect and prevent malicious traffic.  
- Testing network connectivity, troubleshooting firewall and IDS configuration issues.  
- Practicing operational security by ensuring internet access was restored after firewall installation.  
- Documenting findings and configurations for reporting.  
  
Challenges encountered:  
  
- Initial confusion with selecting appropriate network adapter types and assigning them to WAN and LAN interfaces.  
- Difficulty navigating the pfSense web interface for advanced configuration options.  
- Managing firewall rules to avoid blocking legitimate traffic while preventing unauthorized access.  
- Troubleshooting issues with IDS/IPS alerts and rule updates.  
- Understanding how to effectively test firewall and IDS functionality using attack simulations.  
  
Key learnings:  
  
- The importance of accurate network interface mapping in virtual environments.  
- How to create granular firewall rules to control traffic flow.  
- Integration of IDS/IPS enhances network security by providing real-time monitoring and threat prevention.  
- Testing firewall and IDS configurations requires iterative troubleshooting and validation.  
- Documenting configuration steps and test results is crucial for operational handover and audits.  
  
This lab enhanced my practical skills in firewall management, network security configuration, and intrusion detection, preparing me for real-world cybersecurity infrastructure tasks.