pfSense Frontend Practice – Hands-On Assignment & Assessment Document

Student Submission: Complete 4 out of 8 Lab Exercises

Overview

This hands-on assignment is designed to strengthen practical skills in pfSense WebGUI administration.
Students must perform configuration, verification, and documentation tasks across networking, firewalling, DHCP, DNS, NAT, VPN, and traffic shaping.

Each lab provides a **scenario**, followed by **mandatory tasks** that students must complete without hints.
Students are evaluated on accuracy, completeness, screenshots, and clarity of observations.

Submission Requirements (For Students)

✓ Submit **any 4 labs out of the 8**
✓ Each lab must include:

- Required screenshots
- Observations/explanations
- Description of configuration logic
  ✓ Use a single PDF or doc file
  ✓ File naming format: **Name_Batch_pfsense_Assignment.pdf**

LAB 1 – Networking & Interface Configuration

Scenario:

Your pfSense firewall has multiple physical and virtual interfaces attached. You have been asked to standardize interface naming, configure the internal network, and ensure consistent behavior after reboots.

Tasks:

1. Identify all physical and virtual interfaces visible to pfSense.
2. Configure one interface as **LAN** with a static private IP address range (student chooses /24, /25, etc.).
3. Rename *all* interfaces with meaningful names (LAN-Core, WAN-Uplink, Lab-Network, etc.).
4. Reboot pfSense and confirm all changes persist.
5. Modify MTU on any one interface and document:
   - where the MTU change is reflected in the GUI
   - how it impacts connectivity
6. Disable one unused interface and describe traffic behavior before and after disabling.

Assessment Deliverables:

- Screenshots of interface list, LAN config, MTU change location
- Short explanation of traffic behavior when disabling an interface

LAB 2 – Firewall Rule Logic & Policy Enforcement

Scenario:

Your network requires targeted access control and monitoring. You must enforce selective permissions and visibility for troubleshooting.

Tasks:

1. Create a firewall rule that permits traffic for **one specific internal host only**.
2. Block **all ICMP traffic** originating from LAN.

3. Create a **time-based rule** allowing traffic only during working hours (students define timeframe).
4. Enable logging on a deny rule and identify where logs appear in the pfSense GUI.
5. Capture which firewall rule matches a blocked packet and document how you determined it.

Assessment Deliverables:

- Screenshot of rule list with time-based rule
- Evidence of blocked ICMP
- Screenshot from firewall logs showing matched rule
- Short written explanation of rule match logic

LAB 3 – NAT & Port Forwarding

Scenario:

You must configure outbound NAT behavior and set up selective port forwarding for a hosted application.

Tasks:

1. Identify the NAT mode currently operating (automatic/manual/hybrid).
2. Configure **outbound NAT** for one internal subnet only.
3. Set up a **port forward** from WAN to an internal service (student chooses service/port).
4. Prevent internal users from accessing the forwarded service using the public IP (NAT reflection handling).
5. Observe and document active NAT translation states.

Assessment Deliverables:

- Screenshot of NAT mode
- Screenshot of outbound NAT entry
- Port forward screenshot
- Screenshot of NAT states table
- Explanation of how NAT reflection was prevented

LAB 4 – DHCP Server & Client Policy Control

Scenario:

You must prepare the LAN for automated addressing, device control, and DNS customization.

Tasks:

1. Enable DHCP on LAN and create a valid IP pool.
2. Reserve a **static DHCP mapping** for one device.
3. Configure **custom DNS servers** for DHCP clients.
4. Block all **unknown/unauthorized** devices from receiving IP addresses.
5. Locate active DHCP leases and document:
   - hostname
   - MAC
   - assigned IP
   - lease status

Assessment Deliverables:

- DHCP pool screenshot
- Static mapping screenshot
- DHCP lease table
- Short note on how unauthorized device control was enforced

LAB 5 – DNS Resolver & DNS Control

Scenario:

Your organization wants to centralize DNS handling and restrict certain domain resolutions.

Tasks:

1. Verify whether pfSense is currently using **DNS Resolver** or **DNS Forwarder** mode.
2. Create a **custom hostname override** that resolves only inside LAN.
3. Enable **DNSSEC** and document how validation failures are reported.
4. Block resolution of selected domains (e.g., social media) for LAN clients.
5. Observe DNS query flow using pfSense diagnostics and summarize behavior.

Assessment Deliverables:

- Screenshot of DNS mode
- Host override entry
- Screenshot showing DNSSEC validation failure
- Domain block test evidence
- DNS diagnostics observation summary

LAB 6 – Traffic Shaping & Rate Limiting

Scenario:

Network performance must be optimized to prioritize key applications while controlling excessive bandwidth usage.

Tasks:

1. Determine real-time bandwidth usage per interface.
2. Apply a **bandwidth limit** to a specific host/IP.
3. Prioritize **interactive traffic** (SSH/VoIP) over bulk downloads.
4. Observe and document packet behavior when traffic exceeds limits.
5. Test new connections during congestion and describe behavior.

Assessment Deliverables:

- Screenshot of bandwidth usage
- Rate-limit rule screenshot
- Observations on traffic queue behavior
- Notes on new-connection behavior under congestion

LAB 7 – VPN – Secure Remote Access

Scenario:

Your task is to establish secure remote access for team members using pfSense's supported VPN technologies.

Tasks:

1. Identify all **supported VPN types** visible in pfSense WebGUI (OpenVPN, IPsec, WireGuard, etc.).
2. Configure a **remote access VPN** (student chooses technology).

3. Assign an **IP address pool** for remote clients.
4. Restrict VPN clients so they only access **limited internal resources**.
5. Verify tunnel status, connected clients, and connection parameters.

Assessment Deliverables:

- VPN configuration screenshots
- Address pool configuration
- Firewall rule restricting VPN traffic
- Screenshot of status/connected clients

LAB 8 – Integrated Policy Exercise (Advanced)

Scenario:

This exercise integrates multiple pfSense components into a cohesive enterprise-style configuration.

Tasks:

1. Design interface separation for **Management**, **LAN**, and **WAN** networks.
2. Restrict VPN users to **limited DNS + HTTP only**.
3. Configure **rate limits** on a Guest network that differ from internal LAN limits.
4. Provide **DHCP only to trusted devices**, blocking all others.
5. Observe the **state table** during simultaneous NAT + VPN traffic and summarize patterns.

Assessment Deliverables:

- Diagram or screenshot of interface assignments
- Rules restricting VPN traffic
- Guest network shaper rules
- DHCP allow-list configuration
- Screenshot of state table + analysis summary