Enterprise Infrastructure SOC Lab (2025)

Firewall, Identity, VPN, Access Control, Visibility — designed, implemented, and proven in a controlled lab.

This project replicates a corporate environment to demonstrate **security engineering fundamentals**: designing, implementing, breaking/fixing, and proving the core security controls that a SOC or Security Engineer relies on.

Executive Summary

- Built a miniature enterprise with **pfSense firewall + VPN**, **Windows Server 2019 (AD DS, DNS, DHCP, File Services)**, **Windows 10 client**, **Ubuntu client**, and **Kali attacker**.
- Validated end-to-end **identity, access control, perimeter defense, and detection visibility**.
- Captured **hard evidence** (screenshots + packet captures) to prove configuration and security controls.

Architecture

- **pfSense** → Firewall, NAT, VPN Gateway (`192.168.100.1`)
- **SRV-CORE** → Domain Controller, DNS, DHCP, File Server (`192.168.100.10`)
- **WIN10-CLI** → Domain workstation + Wireshark endpoint
- **UBU-CLI** → Linux client (routing/DNS drills)
- **KALI-ATT** → Attacker (nmap, brute-force, tcpdump)
- **VPN** → OpenVPN tunnel (`10.8.0.0/24` → corporate LAN route)

*Diagram available in repo: *`docs/diagram_lab_topology.png`

Security Objectives

1. **Perimeter Control** → pfSense firewall enforces rule order, logs blocked traffic.
2. **Identity & Authentication** → Active Directory with Kerberos tickets validated on client and DC.
3. **Access Control** → Group-based NTFS permissions (AGDLP) on hidden share `Finance$`.
4. **Remote Access** → VPN tunnel provides secure, controlled access to LAN.
5. **Visibility & Detection** → Sysmon telemetry, Windows audit policies, Wireshark captures.

Implementation Highlights

1. Networking – DHCP & DNS

- **Problem:** Without DHCP/DNS, clients fall to APIPA (`169.254.x.x`) and domain resolution fails.
- **Action:** Configured DHCP scope + DNS zone; captured **DORA handshake** and `nslookup` to prove.

- **Evidence:** `dhcp_dora_wireshark.png`, `dns_nslookup_srv_lab_local.png`

2. Firewall Enforcement

- **Problem:** Needed proof firewall rules enforce in order.
- **Action:** Added pfSense ICMP block rule above allow-any.
- **Evidence:** `pfsense_firewall_log_icmp_blocks.png`

3. Identity & OUs

- **Problem:** GPOs do not apply to default *Computers* container.
- **Action:** Created **Workstations OU**, moved WIN10-CLI into it.
- **Evidence:** `aduc_ous_with_win10-cli_in_workstations.png`

4. Access Control – Finance Share

- **Action:** Created hidden share `Finance$`, applied group `GG_Finance_RW`.
- **Evidence:**
- Alice access allowed → `financeshare_alice_access.png`
- Bob denied → `financeshare_bob_access_denied.png`

5. Kerberos Authentication

- **Action:** Captured Kerberos **TGT + TGS** using `klist`; validated DC logs (4768/4769/4624).
- **Evidence:** `klist_before.png`, `win10-cli_klist_tgt_tgs.png`, `eventviewer_security_4768_4769_4624.png`

6. VPN Access

- **Action:** Configured pfSense OpenVPN; pushed route to LAN; verified share only reachable via VPN.
- **Evidence:** `pfsense_openvpn_status_connected.png`

7. Visibility – Sysmon + Brute Force

- **Action:** Installed Sysmon, simulated brute-force via Kali Hydra.
- **Evidence:**
- Sysmon process creation → `sysmon_eventid1_process_creation.png`
- 4625 failed logons → `eventviewer_security_4625_failed_logons.png`

Break → Symptom → Fix

- DHCP stopped → Clients get APIPA → Restart DHCP service → Renew lease.
- DNS wrong → `srv.lab.local` fails → Reset DNS to DC (`192.168.100.10`).
- No gateway → LAN OK, Internet dead → Restore pfSense `.1` as GW.
- Kerberos fail → Time skew > 5 mins → Resync NTP, correct DNS.
- Firewall order → Block below allow-any ineffective → Move block above.

Detection Scenario

- **Baseline:** Normal Kerberos ticket issuance validated (`klist`, DC logs).
- **Attack:** Kali brute-force generated a 4625 logon storm.
- **Response:** Correlated Sysmon Event ID 1 (powershell.exe) with failed logons.
- **Outcome:** Proved end-to-end visibility from endpoint → DC → firewall.

Lessons Learned

- DNS is the backbone of AD authentication.
- Firewall rule **order** determines security enforcement.
- Group-based access (AGDLP) is scalable; per-user ACLs fail.
- Packet captures validate what logs only imply.
- Visibility via Sysmon + audit policy is mandatory for brute-force detection.

Skills Demonstrated

- **Identity & Access:** AD DS, Kerberos, NTFS, OUs, Groups
- **Networking:** DHCP, DNS, NAT, routing, VPN
- **Perimeter:** pfSense firewall, rule design, logging
- **Endpoint Visibility:** Sysmon telemetry, Windows audit policy
- **Detection Engineering:** Brute-force & Kerberos monitoring
- **Troubleshooting:** Break/fix drills under pressure

Ethics

All offensive tools (nmap, brute-force) were executed only in an **isolated lab environment**. No production systems were targeted.

ISO/IEC 27001:2022 Control Mapping

Enterprise Infrastructure SOC Lab — Controls covered and where they’re evidenced in the lab.

ISO Control	Lab Coverage
A.5.15 – Access Control	Enforced via pfSense firewall rules, VPN access, and NTFS permissions on Finance$ share (AGDLP model).
A.8.2 – Identity Management	Active Directory domain accounts, OUs, Kerberos authentication.
A.8.3 – Authentication Information	Logon validation, password use, Kerberos ticketing.
A.8.15 – Logging	Sysmon telemetry, Windows Event Logs, pfSense firewall logs.
A.8.16 – Monitoring Activities	Continuous detection of brute-force login attempts (4625 storms, Sysmon Event ID 1).
A.8.17 – Clock Synchronisation	Resolved Kerberos time skew issues with NTP sync.
A.8.20–22 – Network Security / Services / Architecture	pfSense firewall, VPN tunnel, NAT, secure routing.
A.8.23 – Segregation of Networks	VPN-only access to LAN, separation of attacker subnet.
A.8.9 – Configuration Management	Break→Fix drills on DNS, DHCP, firewall ordering.
A.10.1 – Continual Improvement	Documented lessons learned, iterative fixes.