

Forum: [Hack Forums](#)

Thread: [Network Security: Segmentation, ACLs & Hardening](#)

Vectura - October 2, 2025, 4:04 pm

Network Security: Segmentation, ACLs & Hardening

Intro:

This tutorial shows practical, legal techniques for segmenting networks, configuring a small pfSense gateway, and implementing VLANs and ACLs — perfect for home labs and SMB environments.

Prerequisites: pfSense VM or physical device

Managed switch supporting VLANs (or virtual switches)

Basic networking knowledge (IP, subnetting)

Guide:

Design network zones

- Example: Guest Wi-Fi 192.168.50.0/24, Workstations 192.168.10.0/24, DMZ 192.168.20.0/24

pfSense basic config

Code Interfaces: WAN (DHCP/NAT), LAN (192.168.10.1/24), OPT1(DMZ 192.168.20.1/24)

NAT: enable outbound NAT for internet access

Firewall rules: default deny, allow only required ports

Create VLANs on switch and trunk to pfSense

- Configure trunk and access ports per VLAN

Implement ACL rules

- Deny guest -> internal, allow internal -> internet

Monitor & log

- Enable firewall logs and central logging

Exercises: Setup two VLANs and verify isolation via ICMP/tcpdump

Create a rule that allows a single server to reach internet only on ports 80/443

Note: do not expose management interfaces to the open internet without MFA and access controls.