Virtual Internship Program 2025 — Cyber Security Stream

Cyber Shield: Defending the Network

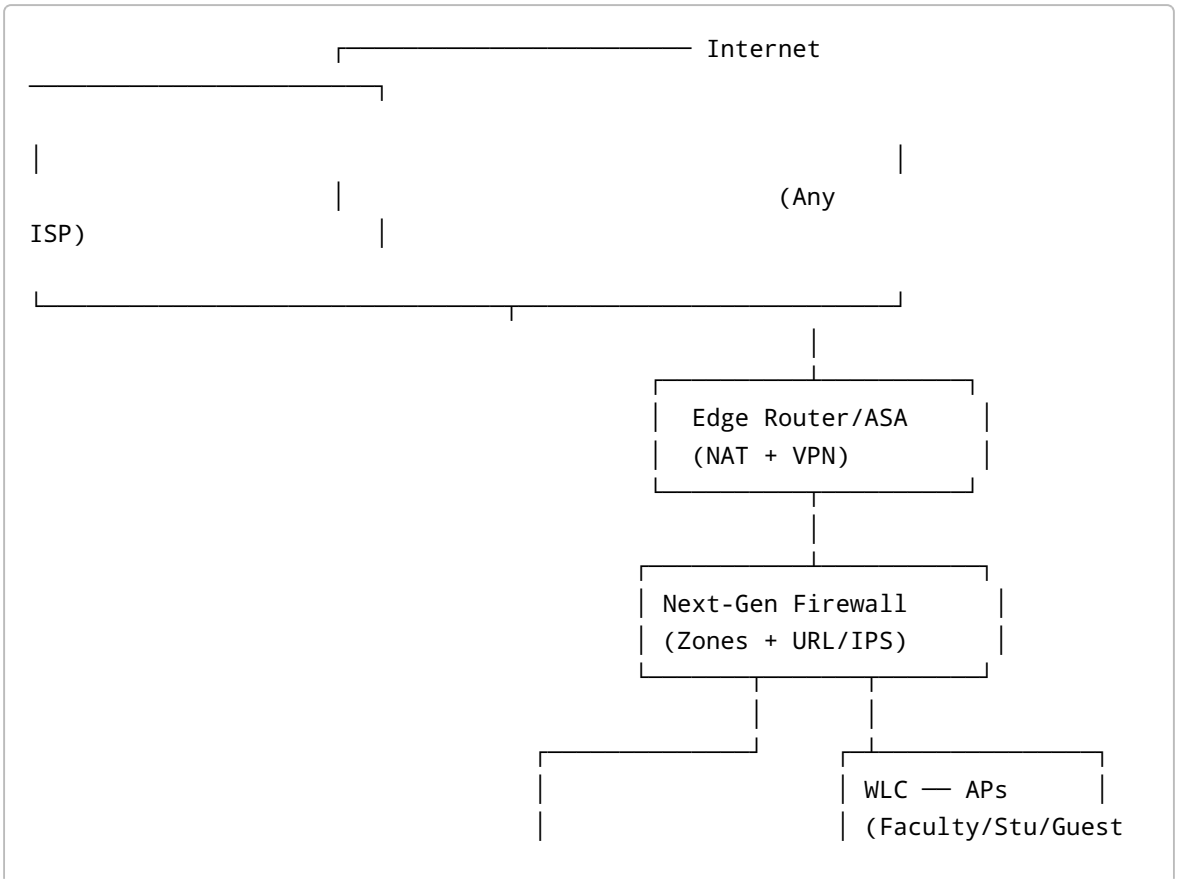
Submitted by: Aarav Raj\
aaravraj8292@gmail.com **Contact:** +91 8969106223 **Email:**

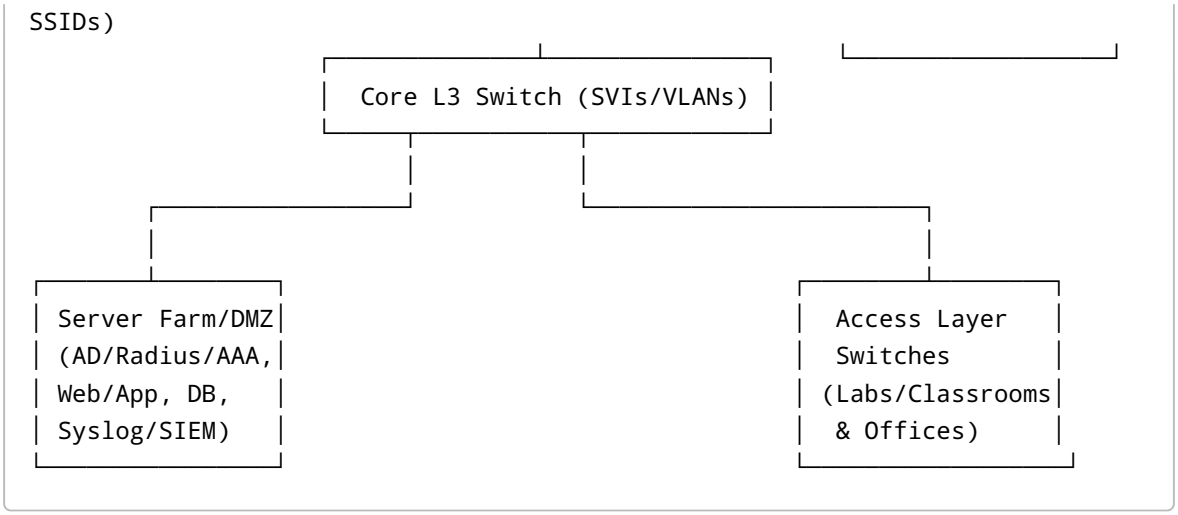
PART 1 — Internal Red-Team Style Audit of College Network

1) Scope & Objectives

- Map the current campus network using Cisco Packet Tracer (routers, L3/L2 switches, firewalls, wireless controllers/APs, servers, endpoints).
- Identify trust zones and segmentation boundaries (User VLANs, Server VLANs/DMZ, Management, Guest, IoT).
- Inventory current security controls (ACLs, firewall rules, WPA2/WPA3-Enterprise, 802.1X, AAA, IDS/IPS, NAC, logging/SIEM).
- Perform attack-surface mapping and propose risk-based mitigations fit for tight budgets and limited staff.

2) Assumed Reference Topology (to be replicated in Packet Tracer)





Trust Zones (examples):

- **Mgmt:** out-of-band mgmt, AAA, logging.
- **Server/DMZ:** AD/LDAP/RADIUS, app/web, DB, updates, proxy.
- **Faculty:** wired/wireless VLAN with higher privileges to academic tools/research repos.
- **Student:** wired/wireless VLAN with restricted east–west access.
- **Guest/IoT:** strict egress, no lateral movement; captive portal for guests.

3) Attack Surface Mapping (sample findings)

- **Flat network segments** enabling lateral movement between Student and Faculty VLANs.
- **Weak WLAN auth** on legacy SSID (WPA2-PSK) → upgrade to 802.1X (EAP-TLS/PEAP).
- **Missing NAC posture** → unmanaged/compromised devices connect freely.
- **Coarse ACLs** at L3 SVI; server subnets reachable from user VLANs beyond required ports.
- **Limited DNS control** → phishing/C2 resolution possible; no egress DNS policy.
- **Sparse logging** and no alerting on critical changes.

4) Recommended Controls (budget-aware)

- **Segmentation:** Per-VLAN ACLs and inter-VLAN firewalling for Student↔Faculty↔Server; block east–west by default; allow only required ports.
- **802.1X + Central AAA:** RADIUS-backed 802.1X for wired/wireless; group-based policy.
- **NAC:** Device profiling & posture checks (quarantine/remediation VLANs).
- **DNS-layer security:** Protective DNS for phishing/malware & category policies.
- **Least-privilege server access:** Jump host/Bastion, RBAC, service allowlists.
- **Logging/SIEM:** Central syslog, NTP, alerts; weekly review.
- **Patch & Backup hygiene:** Monthly patch window; config backups; golden images.
- **User awareness:** phishing drills; short “click-hygiene” modules.

5) Part-1 Deliverables (to include in submission)

- **Packet Tracer .pkt** file of the mapped campus network (with labels and VLANs).
- **Network topology diagram** (exported PNG from Packet Tracer).
- **Security assessment report** (this document) with risks + mitigations and an attack-surface table.

PART 2 — Secure Hybrid Access (Faculty from anywhere; students from personal devices)

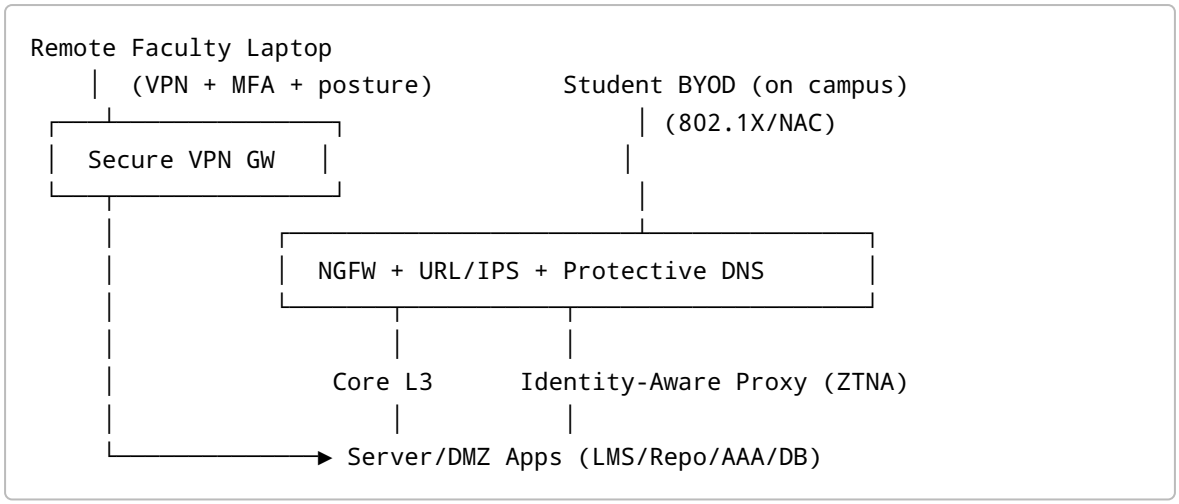
1) Design Goals

- **No direct internet exposure** of internal apps.
- **Role-based access:** Faculty vs Student policy separation.
- **Simple to run:** lean IT team; reuse current gear.
- **Scalable & secure:** supports peak loads/exams and remote faculty.

2) Chosen Building Blocks

- **Remote Access VPN client** for faculty laptops with posture checks.
- **ZTNA/Identity-aware proxy** for selected web apps (portal/LMS) to reduce VPN load.
- **NAC + 802.1X** on campus for both wired/wireless with role-based VLAN assignment.
- **Protective DNS** for all user traffic on- and off-campus.
- **Strong MFA** for all remote and privileged access.
- **Split-tunneling** only for low-risk SaaS; force-tunnel for internal services.

3) Updated Hybrid Topology (high-level)



4) Policy Model & AuthN/AuthZ Flows

- **Faculty (remote):** Duo-MFA → VPN posture (AV/patch) → role = Faculty → permitted apps (LMS, repo, research) via allowlist; SMB/SSH via jump host only.
- **Faculty/Student (on campus):** 802.1X (user cert or creds) → NAC profile → VLAN/SGT assignment (Faculty/Student/Guest) → DNS policy + egress ACLs.
- **Students (remote):** Web access to LMS via identity-aware proxy + MFA; no network-level access to internal subnets.
- **Admins:** Privileged access via VPN + PAM jump host, session recording; no direct RDP/SSH from internet.

5) Risks, Trade-offs & Fallbacks

- **VPN concentration** can bottleneck → size gateway modestly; enable split-tunnel for SaaS only; secondary standby gateway.
- **ZTNA/i-aware proxy complexity** → start with LMS/portal; expand iteratively.

- **NAC tuning effort** → phase rollout, start with profiling/monitor-mode, then enforce.
- **User friction with MFA** → remember-me on managed devices; offline codes for faculty.

6) Part-2 Deliverables

- **Updated network diagram** showing VPN gateway, ZTNA/IAP, NAC, MFA, DNS enforcement and policy zones.
- **Technical note**: components, auth flows, risks, roll-out plan, and operating procedures.

Appendices

A. Sample VLAN/ACL matrix (to be tailored to actual subnets/ports).\ **B. Sample DNS filtering policy categories for Student/Faculty/Guest.**\ **C. Ops checklists:** daily/weekly tasks, patch windows, backup schedule.

End of Document.