
**Department of CSE-IoT**

**Lakshmi Narain College of Technology, Bhopal (M.P.)**

# Cisco AICTE Virtual Internship Program 2025

A Cisco AICTE Virtual Internship project report on Cyber Security Submitted in partial fulfilment of the requirements for the AICTE-CISCO virtual internship in Cyber Security Program 2025.

Submitted By: Divya Arya

| | | |
|---|---|---|
| **AICTE Internship Student registration ID** | **:** | STU644953d0b07ba1682527184 |
| **Student ID (Enrolment Number)** | **:** | 0103IS221071 |
| **Email** | **:** | divyarya06@gmail.com |

**Problem Statement for Cyber Security stream**

**Cyber Shield: Defending the network**

# Problem Statement for Cyber Security Stream:

**Cyber Shield: Defending the network**

**Part 1:**

Problem Statement: You are a part of the cybersecurity student team at your college, freshly enrolled in the Cisco NetAcad Cybersecurity course. With access to Cisco Packet Tracer and your growing knowledge of security fundamentals, you've been given your first real-world challenge.

Your task is to analyze your own college network as if you were part of an internal red team. You'll begin by mapping the current infrastructure using Cisco Packet Tracer, identifying devices, access points, firewalls, segmentation boundaries, and any existing security controls.

But this isn't just a drawing exercise. You are expected to assess how effective these controls are in today's threat landscape. Where are the weak points? Are there flat zones that allow lateral movement? What would an attacker target first, and how would you stop them?

Using the knowledge from your NetAcad course and insights gained through simulation, conduct an attack surface analysis, and present your findings. Your recommendations should reflect real-world thinking: assume budgets are tight, staff are limited, and security is everyone's afterthought until something breaks.

Tasks:

- Conduct a complete analysis of the existing college campus network layout, devices, and zones.
- Use Cisco Packet Tracer to create a visual representation of routers, switches, firewalls, and access points.
- Assess how the network is segmented and which trust zones exist.
- Identify and document any security controls such as firewalls, IDS/IPS, authentication servers, or ACLs.
- Perform an attack surface mapping exercise to locate potential weaknesses.
- Suggest risk-based countermeasures, policy changes, and improved control placement

Deliverables:

- A detailed network topology diagram highlighting infrastructure, zones, and attack surface.
- Security assessment report highlighting identified security risks, suggested solutions and countermeasures to mitigate attack surfac

**1) Current network – simple picture**

**Your college network already has some separation between groups:**

- **Labs (wired only) – PCs are connected by Ethernet, and they cannot talk to each other directly.**
- **Teachers' offices – Teachers have personal PCs that can use Ethernet or a teachers-only Wi-Fi.**
- **Placement Department – Their own Wi-Fi and Ethernet. Phones can also connect to the college Wi-Fi.**
- **Finance Department – Their own Wi-Fi and Ethernet. Wi-Fi password is sometimes given to outsiders for payment purposes.**
- **Main Network – Internet connection, switches, and maybe some firewall rules.**

---

**2) What's good and what's risky**

**Good points:**

- **Labs already block PC-to-PC communication, so viruses or cheating are harder.**
- **Departments have their own Wi-Fi networks, so normal users can't easily hop between them.**

**Risks:**

1. **Finance Wi-Fi password gets shared → outsiders might use it later for bad purposes.**
2. **Personal devices (BYOD) on Finance/Placement Wi-Fi can bring viruses or hacking tools inside.**
3. **Teachers can connect personal laptops to their VLAN → possible security risk if those laptops are infected.**
4. **Inside each department, devices can usually talk to each other freely → if one gets hacked, it can spread.**
5. **No strict identity check on Wi-Fi (if using shared password) → hard to know who did what.**

---

**3) How an attacker might get in**

- **A visitor gets the Finance Wi-Fi password and tries to hack other parts of the network.**
- **A teacher's personal laptop is infected and attacks internal services.**
- **Someone sets up a fake Wi-Fi with the same name to steal passwords.**
- **Someone inside plugs in a malicious device and sends fake network information.**

---

**4) How we can split the network better**

**We make VLANs (virtual networks) based on roles and devices:**

- **Lab VLAN – for students in labs, only Internet access, no PC-to-PC.**
- **Teacher VLAN (LAN) – for teachers' wired devices.**
- **Teacher Wi-Fi VLAN – same rules as above, for wireless.**

- **Placement VLAN – for Placement office wired and wireless devices.**
- **Finance Staff VLAN – for Finance staff only.**
- **Finance Guest VLAN – for outsiders making payments (different from staff VLAN).**
- **Server VLAN – for internal college servers and applications.**
- **Management VLAN – for controlling switches, routers, and access points.**
- **DMZ VLAN – for public-facing portals (reverse proxy to internal servers).**

---

**5) Access rules in plain language**

- **Labs – Internet only. No access to internal systems or other lab PCs.**
- **Teachers – Access to specific internal apps (portal, ERP), printers, and Internet. No access to Finance or student networks.**
- **Placement – Access to placement tools, email, and Internet. No access to Finance VLAN.**
- **Finance Staff – Access to finance systems, payment gateways, and business websites. Block student/teacher/placement VLANs.**
- **Finance Guest – Internet only, limited to payment sites. No access to any internal systems.**
- **Servers – Only allow the connections they need. Admin access only through the Management VLAN.**
- **Management VLAN – Only for admins managing network devices. No access to user networks.**

---

**6) Low-cost ways to make it happen**

- **Use VLANs with ACLs (Access Control Lists) to allow/block certain traffic between them.**
- **Keep lab PCs isolated like they already are.**
- **Enable security features on switches:**
  - **DHCP Snooping – blocks fake DHCP servers.**
  - **ARP Inspection – stops attackers from pretending to be another device.**
  - **IP Source Guard – blocks devices pretending to have a different IP.**
- **Disable unused ports and lock each port to only one or two allowed devices.**
- **For Wi-Fi:**
  - **Use different SSIDs for each role.**
  - **Prefer WPA2 Enterprise (with username/password) instead of shared password.**
  - **For Finance Guest Wi-Fi, use a voucher system with time-limited passwords.**

---

**7) Policy changes (easy but powerful)**

- **Stop sharing the same Wi-Fi password for Finance with outsiders. Use guest Wi-Fi with time-limited codes.**

- **Rotate passwords regularly (Wi-Fi, device admin passwords).**
- **BYOD rules – devices must be updated, have screen lock, and be isolated from other users on Wi-Fi.**
- **Guest devices – can only connect to guest network, never to staff networks.**

---

**8) Examples of problems and fixes**

- **Finance password leaked → move to voucher guest network, block access to internal IPs.**
- **Teacher laptop infected → limit teacher VLAN to only allowed apps and Internet.**
- **Fake Wi-Fi attack → train staff and use per-user login.**
- **Malicious device in lab → use switch security features to block it.**

---

**9) Simple starting firewall rules**

- **Finance Guest → Internet only, no private IPs.**
- **Labs → Internet only.**
- **Teachers/Placement → Only web access to allowed internal apps and Internet.**
- **Finance Staff → Access to finance systems, restricted Internet.**
- **Management → Only device administration access.**

---

**10) Light monitoring plan**

- **Collect logs from switches, routers, and APs for security alerts.**
- **Check daily if guest network is being misused.**
- **If Wi-Fi password is leaked → change it immediately or disable SSID.**
- **If a device is infected → put it in a quarantine VLAN until it's fixed.**

**PART 2:**

Problem Statement: After your impressive audit in Part 1, the college IT department has invited you to contribute to a new project: enabling a hybrid access model for students and faculty.
Faculty members will now work flexibly from home or campus, and require uninterrupted, secure access to teaching tools, research repositories, and internal services. Students, on the other hand, will continue using personal devices to access shared academic portals and lab resources.
But here's the catch: the administration has made it clear that the internal services must never be exposed directly to the internet.
Your task is to design a secure hybrid network architecture that supports remote access while enforcing strict boundaries. Think like a network engineer and evaluate options like VPN, SASE, identity-aware proxies, or split tunneling. Consider not only how to connect, but how to ensure the right people access the right services at the right time.
Can your design balance simplicity, security, and scale without overwhelming the existing infrastructure?

Tasks & Deliverables:

- Design network segmentation based on user roles (faculty vs student).
- Recommend secure access tools like VPN, SASE, identity-aware proxies, or split tunnelling.
- Define trust models, authentication flows, and control access to internal apps.
- Update the campus network topology to show remote access pathways, gateways, and policy enforcement zones.
- Justify your architecture with risks, use cases, and fallback strategies.

Deliverables:

- Updated network diagram with new hybrid access components.
- Technical documentation explain

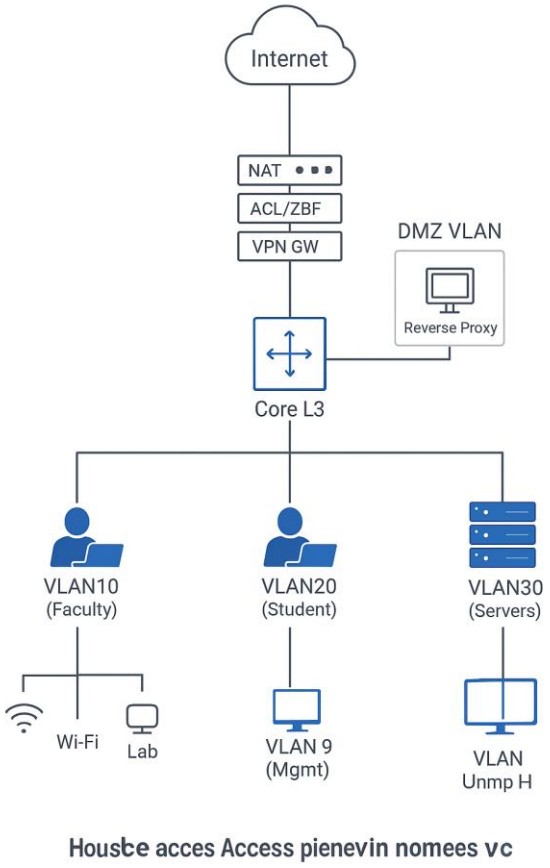
**1) What we're building (in one line)**

A **role-segmented campus + VPN** design where:

- **Faculty** can work from home or campus over a **secure VPN** (with **split tunneling** so only campus traffic goes through VPN).
- **Students** keep using campus Wi-Fi/labs but **only** reach shared portals (never the internal app servers directly).
- All internal apps are reached **through a portal/reverse proxy** in a **DMZ**, not exposed to the internet.

---

1) **Simple high-level diagram (ASCII)**




Housbe acces Access pienevin nomees vc

Key idea: **Students/Faculty → Portal in DMZ (HTTPS) → Internal apps**. Internal servers are never public.

---

**3) Segmentation by roles (keep it simple)**

- **VLAN10 – Faculty (LAN + Faculty-WiFi)**
  Staff laptops/desktops, allowed to reach teaching tools and research via the **portal**.
- **VLAN20 – Students (Student-WiFi + Labs)**
  BYOD and lab PCs; **no device-to-device** in labs; only allowed to the **portal** and internet.
- **VLAN30 – Servers (Internal)**
  App/DB/AAA servers. **Not reachable directly** from students. Access is via portal or jump host.
- **VLAN40 – DMZ (Portal/Reverse Proxy)**
  Public-facing web/portal (HTTPS). Forwards to internal apps on **specific ports only**.

- **VLAN99 – Management**
  Switches/routers/APs and a **jump host** for admins. No user traffic here.

Why this helps: if malware hits one area, it can't easily move sideways (east-west).

---

**4) Secure access options (what to use & why)**

- **Remote access VPN (IPsec)** → for **Faculty** working from home.
  - **Split tunneling**: only campus IPs go through VPN; YouTube/other normal internet stays local. Faster and uses less bandwidth.
- **Identity-Aware Proxy (concept)** → the **portal** checks user identity & role (Faculty vs Student) before forwarding to apps.
  - In Packet Tracer we simulate with a **DMZ Web Server** acting as a **reverse proxy**; in real life, you'd add SSO/MFA.
- **SASE/Cloud ZTNA (future option)** → Mention as a roadmap if college wants cloud-based access control later. Not required for now.

---

**5) Trust model (who trusts whom)**

- **Least privilege**: every VLAN only talks to what it must.
- **Faculty**: can reach portal and specific internal tools (e.g., LMS, research repo).
- **Students**: can reach portal and lab services, but **not** the internal servers directly.
- **Servers**: do **not** initiate to users; only reply and talk to the portal.
- **Mgmt**: only admin/jump host can SSH/HTTPS to devices and servers.

---

**6) How the logins/flows work (plain English)**

**On campus (Faculty or Student)**

1. Connect to your SSID or Ethernet.
2. Open the **Portal (HTTPS)** in the DMZ.
3. Login → portal checks your **identity/role** (Faculty or Student).
4. If allowed, portal **forwards** your request to the internal app server; the server is never directly exposed.

**From home (Faculty only)**

1. Start **VPN** to the college **Edge VPN Gateway**.
2. After VPN connects, you can reach the **Portal** and allowed internal tools.
3. Only campus addresses go via the VPN (**split tunnel**) to save bandwidth and keep home internet fast.

Students do **not** use VPN (they only need shared portals, which are available via the DMZ over HTTPS).

---

**7) Policy summary (super short "who can talk to what")**

- **Students** → Internet OK; **Portal (HTTPS) OK**; **deny** direct to Servers.
- **Faculty on campus** → Internet OK; **Portal OK**; allow only needed internal tools (via portal).
- **Faculty remote (VPN)** → Same as above once on VPN; split tunnel on.
- **DMZ Portal → Servers**: allow only **specific app ports**; **deny everything else**.
- **Mgmt VLAN** → can manage network devices and servers; users cannot enter Mgmt.

---

**8) Where to enforce (so it actually works)**

- **Edge Router/Firewall**:
  - Terminate **VPN**; do **NAT**; apply **ACLs/ZBF** between Internet, DMZ, and Campus.
- **Core L3 (or Router-on-a-Stick)**:
  - **Inter-VLAN ACLs**: implement the "who can talk to what" rules.
- **Access Switches/APs**:
  - **Client isolation** for labs and student Wi-Fi (no device-to-device).
  - **First-hop security**: DHCP Snooping, Dynamic ARP Inspection, Port-Security (stops spoofing/rogue DHCP).
  - Map **SSIDs → VLANs** (Faculty SSID → VLAN10, Student SSID → VLAN20).

---

**9) Risks & how we handle them (simple)**

- **VPN overload** (too many users): use **split tunneling**; add schedules if needed.
- **Portal compromised**: it's in the **DMZ**, with **tight rules** to servers; you can quickly take it offline and use a backup page.
- **Leaked Wi-Fi password**: rotate PSKs regularly; better is **WPA2-Enterprise (RADIUS)** for staff SSIDs.
- **Lateral movement**: blocked by **VLANs + ACLs + client isolation**.
- **Misconfiguration**: keep a **test checklist** (below) and a simple change log.

---

**10) Use cases (to show it meets requirements)**

- **Faculty edits course from home:** open VPN → portal → LMS → success; YouTube streams directly (split tunnel).
- **Student accesses lab materials:** student Wi-Fi → portal → resources; can't reach internal DBs.
- **Research data access on campus:** faculty LAN → portal → research repo; blocked from student VLAN.
- **Admin maintenance:** jump host (Mgmt VLAN) → SSH to devices/servers; not possible from user VLANs.

---

**11) Quick test checklist (you can run after setup)**

- From **Student** PC:
  - ✓ Can open portal & internet
  - ✕ Cannot ping or open internal server IPs
- From **Faculty** PC (campus):
  - ✓ Can open portal & internal app **via** portal
  - ✕ Cannot RDP/SMB to student machines
- From **Faculty (VPN at home)**:
  - ✓ Can reach portal/internal apps; non-campus sites use normal home internet
- From **DMZ portal**:
  - ✓ Can reach app servers on allowed ports
  - ✕ Cannot reach student/faculty subnets
- **Mgmt**:
  - ✓ Can SSH/HTTPS to switches/routers/servers
  - ✕ Blocked from student VLANs as a destination

---

**12) What to show as deliverables**

1. **Updated network diagram** (use the ASCII idea above when drawing in Packet Tracer):
   - Internet → Edge (VPN/NAT/ACL) → DMZ (Portal) → Core L3 → VLANs (Faculty/Student/Servers/Mgmt).
   - Label VPN gateway, ACL/ZBF points, and SSID-to-VLAN mappings.
2. **Technical document** (short, 2–3 pages):
   - **Segmentation plan** (VLANs & purpose).
   - **Access rules** (the policy summary table).
   - **Remote access choice** (IPsec VPN + split tunneling) and why.
   - **Identity/portal idea** (reverse proxy/IAP concept) and why servers stay private.
   - **Risks & fallbacks** (from section 9).
   - **Test checklist** (section 11).

**PART 3:**

Problem Statement: Soon after the hybrid model rolls out, complaints start coming in: students are streaming videos during lectures, torrenting files in labs, and bypassing basic restrictions using browser extensions and proxies.

The administration turns to you again, and this time for a solution that restricts web access smartly, without creating backlash or blocking legitimate research.

You must design a policy framework that considers:

- Who the user is (student, faculty, guest)
- When they're online (class hours, weekends)
- What content they're trying to access (education, social media, games, etc.)

Explore modern filtering tools: DNS-based filtering, L7 firewalls, proxies, and endpoint-based enforcement. Draft simple, understandable rules, but back them with solid policy logic and enforcement mechanisms.

Don't just stop at blocking sites but instead log events, anticipate circumvention attempts, and define how violations should be reported.

Tasks:

- Compare filtering solutions: DNS filtering, Layer 7 firewalls, proxy-based, or client-side enforcement.
- Design policies that vary by user groups, access time, or category.
- Simulate the enforcement using simple commands or pseudo-policies.
- Add components to the network that enforce and monitor these rules.
- Plan logging and alerting for any access violations.

Deliverables:

- Updated topology with filtering appliance or cloud service locations.
- Web access policy document (in natural language or policy syntax).
- Overview of policy intent, enforcement logic, and advantages.

**1) The Problem**

After the hybrid network was set up, new problems appeared:

- Students watch YouTube/OTT during lectures.
- Torrents are being downloaded in labs.
- People bypass restrictions using browser extensions, proxies, or VPNs.

We can't just block *everything*, because:

- Students and faculty still need access to research papers, educational videos, and academic sites.
- Over-blocking will cause frustration and complaints.

So, we need a **smart filtering system** that:

- Changes rules depending on **who** is using the network.
- Changes rules depending on **when** they are online.
- Decides based on **what content** they're trying to access.

---

**2) Comparing Filtering Methods**

Here's a **simple comparison table** of the main options:

| Method | How it Works | Good Points | Limitations |
|---|---|---|---|
| **DNS Filtering** (e.g., OpenDNS, Cloudflare Gateway) | Blocks websites at the domain name level before they load. | Fast, low-cost, works on all devices without software. | Can be bypassed with alternate DNS or VPN unless locked down. |
| **Layer 7 Firewall (Application Firewall)** | Looks at the *type* of traffic (e.g., video streaming, torrent) and blocks it. | Can block categories like "video" or "P2P" even if URLs change. | Needs good hardware, may slow down high-traffic networks. |
| **Proxy Server Filtering** | All web traffic goes through a proxy that enforces rules. | Can log and control exactly what is accessed. | Must force all users through it, else they bypass it. |
| **Client-side Enforcement** (Endpoint software) | Filtering software installed on each device. | Works even outside campus. | Needs installation & management, students can uninstall unless restricted. |

**Our plan** will use **DNS Filtering + Layer 7 Firewall + Proxy** together, so bypassing one still gets blocked by another.

---

**3) User Groups and Time-based Rules**

We'll have different rules based on **who** is connected and **when**:

| User Type | Class Hours | After Class / Weekends |
|---|---|---|
| **Students (Labs)** | Only educational sites, research portals, coding platforms. Block social media, games, torrents, video streaming (except whitelisted educational videos). | Allow more sites but still block torrents, adult content, and malicious sites. |
| **Faculty** | Full access to educational and research sites, YouTube allowed for teaching, no torrents. | Mostly unrestricted except for dangerous/malicious content. |
| **Guests** | Internet only for general browsing and payments. No internal resources. | Same as above. |

---

**4) Content Categories**

We will allow/block based on categories:

☑ **Always Allowed**:

- Academic journals
- E-learning platforms
- Official news websites
- Government portals

🚫 **Always Blocked**:

- Adult sites
- Torrent & P2P
- Hacking/malware sites

⏳ **Blocked During Class Hours** (students only):

- Social media (Facebook, Instagram, Snapchat)
- Video streaming (Netflix, Prime, YouTube except whitelisted channels)
- Online games

---

**5) Enforcement Tools**

1. **DNS Filtering Service** (e.g., Cisco Umbrella / Cloudflare Gateway)
    - Categorize sites and block unwanted categories.
    - Force DNS via firewall rules so users can't change DNS servers.
2. **Layer 7 Firewall** (Next-Gen Firewall like FortiGate or pfSense with pfBlockerNG)
    - Block torrent protocols, block non-HTTPS proxies, detect VPN traffic.
3. **Transparent Proxy** (Squid)
    - All web traffic is routed here for deeper content filtering.
    - Logs every request for auditing.

4. **Endpoint Controls** (for staff laptops)
    - Lightweight software that enforces same rules when outside campus.

---

**6) Example Policy Syntax (Simplified)**

Here's a pseudo-policy to show the logic:

```
# STUDENT VLAN
If time = 08:00–16:00 AND day = Mon–Fri:
   Block categories: SocialMedia, StreamingVideo, Games, P2P
   Allow categories: Education, News, Government
Else:
   Block categories: P2P, Adult, Malicious

# FACULTY VLAN
Always:
   Block categories: P2P, Adult, Malicious
   Allow all others

# GUEST VLAN
Always:
   Allow categories: GeneralBrowsing, Payments
   Block: All PrivateNetworks, P2P, Adult, Malicious
```

---

**7) Updated Topology with Filtering**

- Add **DNS Filtering Service** before Internet gateway.
- Place **Next-Gen Firewall** between Core Switch and Internet Router.
- Configure **Transparent Proxy Server** inside network for HTTP/HTTPS inspection.
- Management VLAN has access to policy dashboard and logs.

---

**8) Logging & Monitoring**

- All blocked requests are logged with **time, user, and site**.
- Daily reports to IT admin showing:
    - Most blocked categories
    - Top attempted bypasses (e.g., VPN connections)
    - Devices triggering multiple violations

- Alerts for:
    - Torrent activity
    - Repeated access to blocked categories
    - VPN/proxy attempts

---

**9) Handling Bypass Attempts**

- Block alternative DNS requests (UDP/TCP 53 except to our DNS).
- Block common VPN ports (OpenVPN, WireGuard, etc.).
- Inspect encrypted traffic with SSL inspection (for school devices).
- If a user repeatedly tries to bypass:
    - Log incident
    - Temporary block Internet for that device
    - Inform faculty/department head

---

**10) Advantages of This Plan**

- **Smart Filtering** – Different rules for students, teachers, and guests.
- **Flexible** – More relaxed after hours, strict during class.
- **Hard to Bypass** – Multiple layers (DNS + Firewall + Proxy).
- **Transparency** – Clear rules and categories so people know what's blocked and why.
- **Evidence** – Logs help in case of disputes or cyber incidents.