# Cyber Shield – Defending the College Network

Name: Karthikeyan M C

College: Sri Sai Ram Institute of Technology

Date: August 14, 2025

Cisco NetAcad Cybersecurity Internship Project Report

# Part 1 – Network Analysis & Security Assessment

## 1.1 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, your first challenge is to analyze the college network from an internal red team perspective. The objective is to map the infrastructure, identify devices, access points, firewalls, segmentation boundaries, and security controls, and then assess their effectiveness against modern threats.

## 1.2 Existing Network Topology

The network topology was designed in Cisco Packet Tracer and consists of core routers, distribution switches, access switches, servers, and wireless access points. The diagram represents departmental segmentation, administrative systems, and internet gateways.

[Insert Network Diagram Screenshot Here]

## 1.3 Infrastructure Components Identified

- Core Router connected to the ISP  
- Firewall providing perimeter defense  
- Core Switch connecting VLANs and distribution layer  
- Departmental Switches (Admin, Faculty, Labs, Library)  
- Wireless Access Points for student and faculty access  
- DNS, Web, and Email servers

## 1.4 Attack Surface Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Risk Level | Possible Exploit | Recommendation |
| No VLAN segmentation | High | Allows lateral movement between departments | Implement VLANs to isolate traffic |
| Default device credentials | High | Unauthorized device control | Set strong unique passwords |
| Open unused ports | Medium | Rogue device access | Disable unused ports, enable port security |
| Lack of ACLs | High | Unrestricted inbound/outbound traffic | Deploy ACLs to filter traffic |
| Unsecured Wi-Fi | High | Wireless intrusion | Use WPA3 and MAC filtering |

## 1.5 Security Recommendations

1. Implement VLANs: At least 4 VLANs (Admin, Faculty, Students, Guests) to contain breaches.  
2. Enforce strong passwords: Use 12+ character passwords with complexity.  
3. Port Security: Restrict MAC addresses on each switch port.  
4. ACL Implementation: Deny unnecessary services and restrict sensitive zones.  
5. Wireless Security: Migrate to WPA3 with enterprise authentication.

## 1.6 Example Risk Impact Calculation

If an unsecured Wi-Fi network is exploited, and 200 student devices are active, with an average data rate of 5 Mbps per device, potential data exfiltration could reach:  
200 devices × 5 Mbps × 60 seconds × 10 minutes = 600,000 Megabits (≈ 75 GB of data) in just 10 minutes.

# Part 2 – Secure Hybrid Access Model

## 2.1 Problem Statement

Following the network audit, the IT department requires a hybrid access model to support faculty working remotely and students accessing resources from campus. The internal services must remain protected from direct internet exposure.

## 2.2 Updated Network Design

The updated topology includes a VPN gateway for secure remote connections, an identity-aware proxy for application-level control, and role-based VLAN segmentation.

## 2.3 Role-Based Segmentation

- VLAN 10: Faculty (Full access to teaching tools and repositories)  
- VLAN 20: Students (Access to academic portals and lab resources)  
- VLAN 30: Guests (Internet only)  
- VLAN 40: Administration (Sensitive data access)

## 2.4 Secure Access Flow

Remote faculty connect via VPN, authenticated by RADIUS, then routed to the Faculty VLAN. Students use campus Wi-Fi with WPA3 authentication, mapped to the Student VLAN.

## 2.5 Risk & Mitigation

Risk: VPN compromise → Mitigation: Multi-factor authentication  
Risk: Identity proxy bypass → Mitigation: Layered firewall rules  
Risk: Increased load → Mitigation: Scalable VPN bandwidth allocation

# Part 3 – Smart Web Access Policy

## 3.1 Problem Statement

After hybrid rollout, students abused network resources by streaming videos and torrenting. The task is to implement user-aware, time-based, and category-specific web filtering.

## 3.2 Filtering Approaches

1. DNS-based filtering (Cloudflare Gateway)  
2. Layer 7 Firewall inspection  
3. Proxy-based filtering  
4. Endpoint agents for high-security zones

## 3.3 Policy Design

- Students: Block social media, torrents during class hours.  
- Faculty: Full access except known malicious domains.  
- Guests: Internet only, strict category filtering.

## 3.4 Enforcement Simulation

Example ACL for blocking social media during class hours:  
access-list 110 deny tcp any any eq 443 time-range CLASS\_HOURS  
access-list 110 permit ip any any

## 3.5 Logging & Alerting

Deploy a SIEM system to log all filtering events, trigger alerts on policy violations, and generate weekly compliance reports.