MANIPAL
ACADEMY of HIGHER EDUCATION
(Institution of Eminence Deemed to be University)

Cyber Shield 2025: Defending the network

An Internship Report for Cisco NetAcad - ***Cybersecurity Program***

Networking Academy

Guided by:

Adesh N D

Associate Professor

School of Computer Engineering

Report by:

- *Name –* ***Harsh J More***
- *Semester –* ***5th***
- *Section –* ***C***
- *Registration No. –* ***220909420***
- *Department –* ***Mechanical Engineering***
- *Location –* ***Manipal, Karnataka, India***

Table of Contents

Executive Summary

This internship report presents the result of Cisco NetAcad Cybersecurity Virtual Internship 2025 with an emphasis on the security posture and modernization of a campus-scale network.

The project was split into three major stages, each tackling a realistic scenario in colleges where finances are limited and security tends to be reactive.

In Part 1, the current campus network was documented using Cisco Packet Tracer and examined for segmentation, boundaries of trust, and security controls in place. Weak wireless encryption, unmanaged lateral access among user zones, and monitoring gaps were areas that came under attack surface assessment. Suggestions included VLAN segmentation based on roles, WPA3-Enterprise Wi-Fi, default-deny access policy, and logging and monitoring with enhanced measures.

In Part 2, a secure hybrid access architecture was established to allow faculty to work remotely as students proceeded with personal devices on campus. The selected architecture integrated VPN with multi-factor authentication, identity-aware proxy for services within, and strict policy enforcement isolating faculty from student access paths. This architecture satisfies scale, simplicity, and cost while guaranteeing that no internal services are exposed to the internet directly.

In Part 3, a web access control framework was developed to address misuse of campus bandwidth. DNS-based filtering combined with Layer-7 policy enforcement was applied, with policies that adapt based on user role, time (class hours vs. off hours), and category of content. Logging, alerting, and anti-circumvention measures were included to ensure accountability without impacting legitimate academic research.

In summary, the internship exposed students to real-world campus-scale cybersecurity issues. The recommended solutions show that low-cost, phased changes can greatly minimize attack surface risks, make secure hybrid access possible, and govern responsible web use.

List of figures

Acronyms and Abbreviations

ACL	Access Control List
BYOD	Bring Your Own Device
CSF	Cybersecurity Framework (NIST)
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoH	DNS over HTTPS
EDR	Endpoint Detection and Response
IdP	Identity Provider
IAP	Identity-Aware Proxy
L7	Layer 7 (Application Layer)
MFA	Multi-Factor Authentication
NAC	Network Access Control
NAT	Network Address Translation
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial-In User Service
SASE	Secure Access Service Edge
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SVI	Switched Virtual Interface
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WPA2/WPA3	Wi-Fi Protected Access 2/3
802.1X	Port-based Network Access Control
DoT	DNS over TLS

Introduction

Description

The Cisco NetAcad Cybersecurity Virtual Internship 2025 allowed me to apply in class what I learned to a virtual campus network. The activities primarily entailed testing how secure the network is, identifying vulnerabilities, and recommending it to be enhanced. I also needed to create a secure remote-access system and formulate rules for safe and equitable web usage within the campus.

Objectives

The primary objectives of this report are:

- To analyze the existing campus network topology and inspect its security.
- To divide users and machines into groups (zones) with the help of Packet Tracer.
- To identify vulnerable points and potential attacks in the network.
- To create a secure means of remote connection for faculty and for students to connect using personal devices (BYOD).
- To propose low-cost remedies that would even function with minimal budget and personnel.
- To establish easy web usage policies that filter out harmful sites but continue to permit research and education.

Scope and Assumptions

The project encompasses the routers, switches, access points, VLANs, servers, and internet connection in the campus network simulated here. Physical security (such as locks or CCTV) and the ISP's network are excluded.

Some of the assumptions that have been made are:

- The network is implemented and tested in Cisco Packet Tracer alone.
- Campus resources such as time, money, and personnel are scarce.
- It is the case with most students that they bring their own devices, so the college cannot control them completely.
- Security concepts have to be simple to manage and work properly in a university environment.
- Internal campus facilities need not be directly exposed to the internet.

Methodology and Tools

The actions followed in this work were:

- Creating the campus network diagram using Cisco Packet Tracer.
- Resonating the design for threats based on an attack surface approach.
- Enumerating and prioritizing threats in terms of their likelihood of occurring and their impact.
- Referring to Cisco NetAcad study guides and standard models such as NIST CSF and Zero Trust.
- Writing basic example policies using firewall rules, ACLs, VLANs, and DNS filters.

This method assisted me in bridging theory and practice and learning how to implement simple yet efficient security enhancements in a campus network.

Part 1 — Campus Network Security Assessment

1.1 Current Topology Overview

The network is built to link various sets of users such as faculty, students, labs, and administrative personnel. It also links with key servers and offers internet connectivity to the entire campus. Within this project, the network is demonstrated on Cisco Packet Tracer with all the primary devices and their interfaces.

At the network edge, there is a firewall and main router that connect the campus to the internet. From the main router, cables run to core switches. The switches then run to distribution switches in various buildings, for example, hostels, classrooms, and labs. Access switches link the end devices like PCs, laptops, and Wi-Fi access points.

It also contains servers for services such as DNS, authentication (LDAP/RADIUS), and software applications required by students and staff. Each of these servers is put into its own server VLAN to make them more secure.

To manage the traffic, the users are segregated based on zones using VLANs. For instance, faculty, students, labs, and guests are put into separate VLANs. The Wi-Fi is split into a secure network (through WPA3-Enterprise with 802.1X login) for students and faculty, and a guest Wi-Fi with internet access alone.

The configuration of all the devices on the network (such as routers and switches) is maintained on a dedicated management VLAN so that normal users are not able to directly access the device configurations.

This overall layout replicates a university campus where thousands of devices and users need to be connected but still secured by grouping them and regulating how they communicate with one another.

1.2 Segmentation and Trust Zones

To secure the campus network, all devices and users must be separated into groups. This is segmentation. Each group, or trust zone, will have varying rules for how they can communicate with other groups. Segmentation ensures that even if a section of the network is breached, the intruder cannot easily move into other zones.

In our setup, the following zones are established:

- Faculty VLAN – for staff and instructor computers. They require access to learning materials and internal servers.
- Student VLAN – for student computers. They would receive internet and learning portals but restricted access to sensitive servers.
- Lab VLAN – for lab computers and experiment computers. This one must not be given open access to the rest of the network in order not to let malware propagate.
- Guest VLAN – for guests and temporary users. They receive only internet connectivity, no access to campus internal resources.
- Server VLAN – all critical servers such as DNS, authentication, and apps are located here. This area operates under the tightest rules.
- Management VLAN – accessed solely by network administrators to set up routers, switches, and firewalls. Regular users are not allowed there.

By dividing the network into such zones, security rules are simpler to implement. Student devices, for instance, do not have a direct connection to the server VLAN, and guests are unable to view anything other than the internet. Faculty and lab traffic are also screened to only offer necessary services. This default-deny rule (deny everything, permit what is necessary) secures the campus better and restricts the damage when an attack occurs.

1.3 Current Security Controls

The network on campus is already protected with some fundamental security. The controls are useful, but they cannot defend against all contemporary attacks.

- Internet-edge Firewall: Prevents unwanted traffic coming in from outside and does NAT.
- Access Control Lists (ACLs): Basic rules on routers/switches to permit or deny certain traffic between VLANs.
- Wi-Fi security: Faculty/Student Wi-Fi utilizes WPA3-Enterprise with 802.1X login. Guest Wi-Fi provides access to only the internet.
- Segmentation using VLANs: Faculty, Students, Labs, Servers, and Guests in different VLANs to limit direct access.
- User authentication: Faculty and staff utilize campus credentials (e.g., RADIUS/LDAP). Students utilize basic login for portals and Wi-Fi.
- Monitoring and logging: Basic logs are sent from devices to a syslog server; time is synchronized via NTP. Device status is accessed via SNMP.
- Device management: Routers and switches are administered with SSH on a different Management VLAN.

These are good beginnings, but they have some holes in them. ACLs are limited, BYOD devices are perilous, and logging is rudimentary. We will break down these weak links further in the next section.

1.4 Attack Surface Analysis

Here are listed the vulnerabilities through which an attacker could access or traverse within the campus network. This is derived from the present configuration and our created zones.

- Loose or flat access across VLANs: When ACLs are not complex, users can still access other zones (e.g., Students to Servers). This facilitates lateral movement once a device is compromised.
- BYOD risk: Phones and student laptops are unmanaged. Malware on a single device can propagate in the labs or attempt to scan other networks.
- Wi-Fi misuse: Weak passwords or shared accounts can lead to misuse even with WPA3-Enterprise. Evil-twin APs or rogue hotspots can deceive users.
- DNS bypass: When clients are using public DNS (8.8.8.8 etc.), they can bypass campus policy and access blocked sites.
- Limited monitoring: Simplistic syslog/SNMP might not pick up on policy infractions, scanning, or persistent auth failures immediately.
- Poor lab segmentation: PCs in the lab usually have tools and file shares in common. If one PC is compromised, it is easy to hit others.
- Management exposure: When the management VLAN is accidentally accessible from user networks, attackers may attempt SSH/HTTP on network devices.
- Obsolete services: Default services or old protocols on servers (e.g., unused ports) create attack surface.
- No device health check: There isn't any NAC or posture check. Rooted or infected phones can connect like regular users.
- Single gateway choke: The path with any any rules for convenience in the firewall becomes the easiest path in.

How an attacker might behave:

- Phish a student → obtain Wi-Fi credentials → connect to Student VLAN → scan for open shares → attempt weak passwords → pivot to a lab PC → attempt to access server subnet.
- Configure custom DNS on device → circumvent campus DNS policy → visit torrents or dangerous websites → download malware.
- Configure evil-twin AP close to hostels → steal credentials → reuse on campus Wi-Fi.

1.5 Findings and Risk Prioritization

Here I categorize the primary issues by risk level. High = fix first. Medium = plan next. Low = monitor.

High

- Lateral movement risk between zones because of straightforward ACLs.
- Bypass of DNS via public resolvers.
- Management access not completely isolated or filtered.
- BYOD devices with no health check.

Medium

- Limited logging and alerting (no central correlation, weak visibility).
- Lab VLAN too open inside itself and to other zones.
- Shared or weak Wi-Fi credentials (user behavior risk).

Low

- Unused services/ports on some servers.
- Inconsistent time sync or logging detail.

1.6 Recommendations and Phased Roadmap

The solutions are scheduled in low-cost, small steps so they may be accomplished by campus IT with no substantial changes.

Phase 1 — Disable HTTP and Telnet (this week)

- Default-deny between VLANs: Block all inter-VLAN traffic by default. Then add allow rules only for necessary flows (e.g., Faculty to App Server ports, DNS/HTTP as required).
- Lock management: Mgmt VLAN should be reachable only from admin PC/subnet. Disable SSH/HTTPS/Telnet off. Use SSH only. Implement strong passwords and disable unused services.
- DNS control: Compel all the clients to use campus DNS by blocking outgoing DNS (53/853) from the user VLANs to the internet. Permit only campus resolver.
- Logging fundamentals: Allow extensive logs on firewall/routers. Forward to a central syslog server. Synchronize all devices with NTP.

Phase 2 — Secure access (next 2–3 weeks)

- Wi-Fi hygiene: Maintain WPA3-Enterprise. Implement per-user credentials. Periodically rotate passwords. Disable shared accounts.
- Lab hardening: Isolate lab VLAN so that it does not touch Student VLAN and only required access to servers. Restrict east-west traffic in labs.
- Policy documents: Create concise rules for acceptable use, admin access, and exception handling.

Phase 3 — Improved visibility and control (1–2 months from now)

- Include identity-based control for faculty (VPN with MFA, designed in Part 2).
- Begin DNS security with categories (scheduled in Part 3).
- Enhance monitoring: Simple SIEM or centralized dashboard to monitor auth failures, DNS blocks, and firewall denies.

Expected outcome

- Attack surface diminishes.

- Lateral movement is difficult.
- DNS bypass is shut.
- Admin access is safeguarded.
- Logs provide early warning indicators.

PART 2 – Secure Hybrid Access

2.1 Design Principles and Requirements

Requirements

- Internal services need to be accessed from home and campus.
- BYOD is still used by students on campus.
- Internal apps should not directly be exposed to the internet.
- Simple and low-cost.

Design principles

- Identity first: Access based on user identity and role.
- Least privilege: Provide only what is required.
- Separate paths: Remote path of faculty is separate from on-campus path of student.
- Inspect and log: All critical steps should be logged.

2.2 Suggested Architecture (VPN + Identity-Aware Proxy)

- VPN Gateway in DMZ: Faculty access from the internet to the VPN gateway.
- MFA + IdP: Faculty access campus Identity Provider (IdP) with MFA to log into VPN.
- Identity-Aware Proxy (IAP) for apps: For web applications, traffic passes through an IAP that verifies user group prior to allowing them in.
- Split roles:

- Faculty remote: Internet → VPN Gateway (MFA) → Firewall → Faculty VLAN → internal applications.
- Students on campus: Access Student Wi-Fi/VLAN → Internet access with restrictions; no access to sensitive internal applications.

- No direct access: Internal apps remain isolated; VPN/IAP alone is accessible from the internet.

Where to put pieces

- DMZ: VPN Gateway, and IAP.
- Server VLAN: App servers, DNS, authentication.
- Faculty VLAN: Traffic arrives here (or a separate "VPN-Faculty" VLAN) after VPN.

2.3 AuthN and AuthZ Flow

- Faculty remote login:
  - User initiates VPN client and provides credentials.
  - IdP challenges with MFA (OTP/app push).
  - On success, VPN allocates an IP in the faculty-VPN subnet.
  - Firewall applies rules based on "faculty group".

- Web app via IAP:
  - User opens app URL.
  - IAP checks IdP login and group.
  - If allowed, IAP forwards to internal app over a secure tunnel.

2.4 Policy Enforcement and Segmentation Updates

- Establish a specific VPN-Faculty subnet/VLAN.
- Firewall rules:
  - Permit Faculty-VPN to required app ports.
  - Block Faculty-VPN to Student/Guest networks.
  - Log all denies.
- Restrict Student VLAN to only internet + permitted portals.
- Make Servers accessible from Faculty-VPN alone and required on-campus areas.

2.5 Risks, Limitations, and Fallbacks

- Risk: Overload on VPN gateway during exams.
  - Mitigation: Restrict simultaneous sessions, capacity planning, split-tunnel only for trusted apps if necessary.
- Risk: Faculty device lost/stolen.
  - Mitigation: Require MFA, limited session timeouts, token revocation option.
- Risk: IdP failure.
  - Fallback: Break-glass local administrator account with limited time-bound usage.
- Risk: Confusion for users.
  - Mitigation: Brief user manual and FAQs.

PART 3 – Web Access Policy and Enforcement

3.1 Solution Options and Rationale

- DNS filtering: Easy, inexpensive, category-based, suitable for all devices.
- Layer 7 firewall/proxy: More control, shuts down apps and protocols, more resource intensive.
- Client-side agent: Most effective on managed devices, does not work well for BYOD.

Chosen mix

- Utilize campus DNS filtering for all (students, guests, faculty).
- Apply L7 firewall/proxy to the student VLAN to filter out heavy categories (torrent, malware, crypto-mining, adult) and to implement time-based rules.

3.2 Policy Design (by user and time)

Students

- Class hours: Block gaming, social media, streaming (except approved ed platforms). Permit education, research, coding websites, cloud documents.

- After hours: Ease social media/streaming slightly, still block torrents and malware.
- Always block: Malware, phishing, crypto-mining, explicit illegal material.

Faculty

- Permit majority of categories for research. Still block malware, crypto-mining, torrents.

Guests

- Strictly internet only with filtering. No access from inside.

3.3 Enforcement Logic (DNS/L7/Proxy) and Anti-Circumvention

- Force campus DNS: Block outbound DNS to internet from user VLANs. Allow only campus DNS resolver.
- L7 firewall/proxy: Apply category rules and time schedules on Student VLAN.
- Anti-bypass:
  - Block public DNS (53 and 853) to internet.
  - Block popular proxy/VPN websites on Student VLAN.
  - Keep an eye out for anomalous DNS trends and excessive connections to popular VPN endpoints.

3.4 Logging, Monitoring, and Reporting

- Log blocks of DNS, L7, and authentication to a master syslog/SIEM.

- Generate rudimentary weekly report: top blocked categories, top block reasons, repeat offenders.
- Alarm on peaks of blocked malware or repeated bypass attempts.

Implementation Artifacts

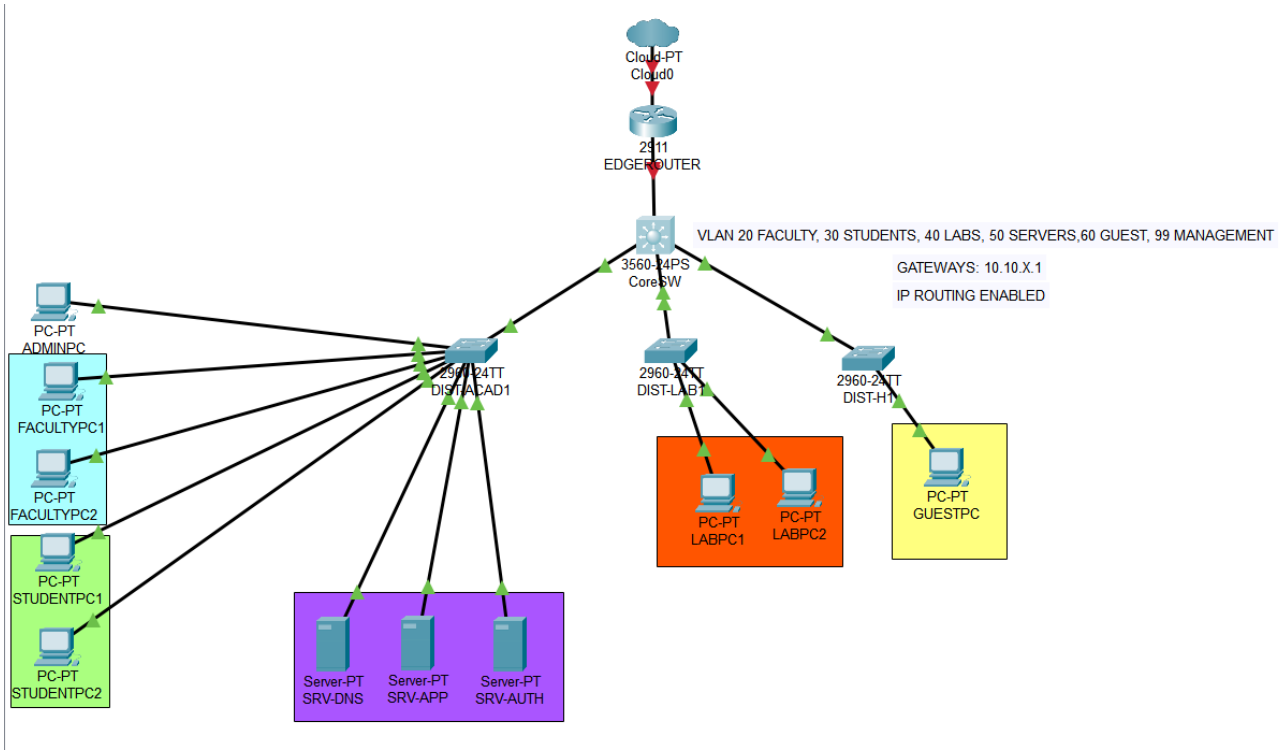

Figure 1

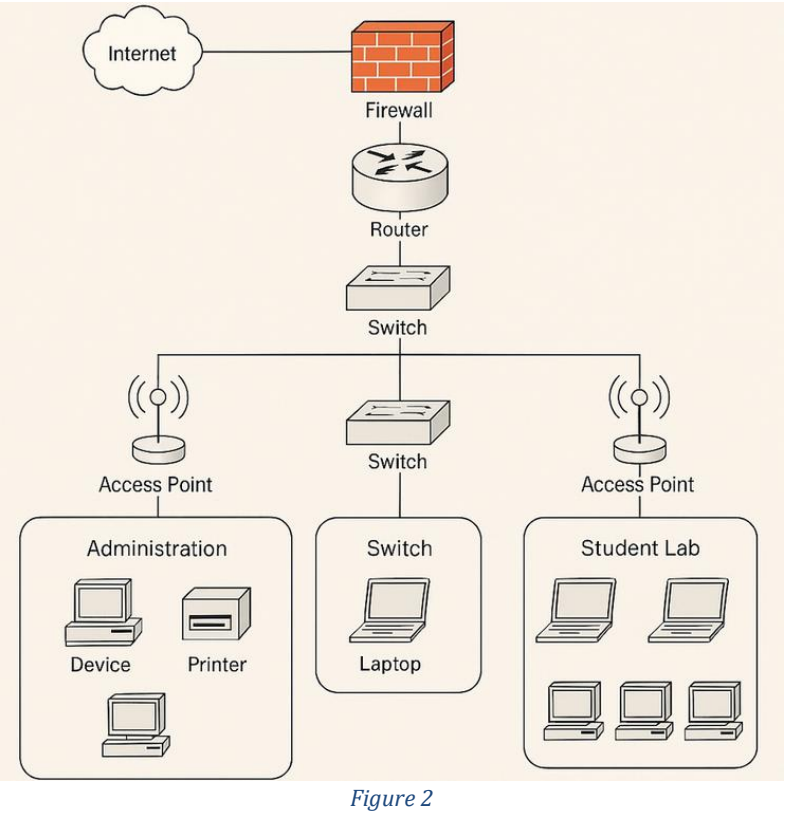

Figure 2

Conclusion

This internship helped me to apply the core concepts of cybersecurity to a college-level network. I first examined the current configuration and pinpointed the most important vulnerabilities like loose controls between VLANs, DNS bypass, and insufficient monitoring. I then suggested small, inexpensive solutions that can be actually deployed on campus: default-deny between VLANs, appropriate management access, enforcing campus DNS, and better logging. Next, I established a general hybrid access architecture with faculty on VPN with MFA and an identity-aware proxy, with students continuing on a separate BYOD path. Finally, I designed web policies that change depending on user and time through DNS filtering and Layer-7 controls with logging and alerts. These steps reduce the attack surface, block easy lateral movement, protect internal apps, and promote responsible web use without inhibiting legitimate study needs. Overall, the project improved my practical experience of employing Packet Tracer and taught me how to balance security, cost, and usability in a university environment.

Acknowledgement

I would like to thank Cisco Networking Academy and AICTE for giving me the chance to learn through the Virtual Internship 2025. I am grateful to our college coordinators and the SPOC for sharing the problem sheet, timelines, and submission steps. I also thank my faculty mentors and lab staff for their guidance and support during the work. Finally, I appreciate my classmates for their help in discussing ideas and reviewing my drafts. Their support made this project easier and more meaningful.

Reference

- Cisco Networking Academy. Introduction to Cybersecurity. Course material.
- Cisco Networking Academy. Cybersecurity Essentials. Course material.
- Cisco Systems. Cisco Packet Tracer Documentation. Product help guide.
- National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), Version 1.1.
- OWASP Foundation. OWASP Top 10 – Common Web Application Security Risks.
- Cisco Systems. WLAN Security Best Practices: WPA2/WPA3-Enterprise and 802.1X.
- Cisco Systems. VLANs and Access Control Lists (ACLs): Configuration and Design Basics.
- Cisco Systems. DNS Security and Layer-7 Policy Concepts (Firewall/Proxy) — Overview guides.