**Final Report: Cyber Shield – Defending the Network**

**Student Name:** Saichandana Nunna  
**College:** Sathyabama Institute of Science and Technology  
**AICTE Internship Student Registration ID** : STU682bf20c6d5001747710476  
**Student ID (Enrolment number)** : 44110548

**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.

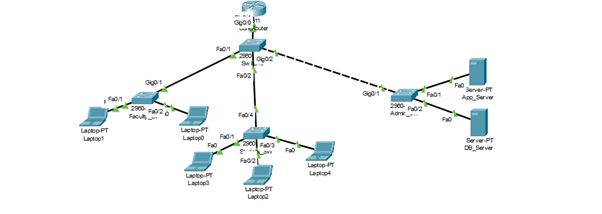
● Suggest risk-based countermeasures, policy changes, and improved control placement

**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 surface risks  
 **Part 1: Network Audit & Attack Surface Analysis**

**1.1 Network Topology Diagram**



***(Packet Tracer file showing the segmented network with the Core Router, Core Switch, and Faculty, Student, and Admin zones)***

**1.2 Security Assessment Report**

**Introduction:**  
This report details the findings of a red team analysis conducted on the college network infrastructure. The assessment aimed to map the network, identify security controls, and locate vulnerabilities.

**Existing Infrastructure & Security Controls:**

* **Network Segmentation:**  
  The network is segmented into three primary VLANs/subnets:
  + Faculty Zone (192.168.10.0/24): High-trust zone for faculty devices.
  + Student Zone (192.168.20.0/24): Low-trust zone for student lab PCs.
  + Admin/Server Zone (192.168.30.0/24): Contains critical services (e.g., LMS, file shares).
* **Security Controls:**
  + A perimeter firewall implemented to filter inbound and outbound traffic.
  + Basic routing ACLs on the core router to enforce inter-VLAN policies.

**Identified Security Risks & Weak Points:**

* Flat Zones: While VLANs exist, no strict ACLs prevent lateral movement.
* Lack of Deep Traffic Inspection: No IPS to block sophisticated attacks.
* Default Configurations: Devices may still use default credentials.
* Single Point of Failure: Core router/firewall is a bottleneck for the entire network.

**Attack Surface Mapping:**  
An attacker would likely target:

* **Student VLAN**: Largest/least privileged zone, prone to phishing/malware.
* **Wireless Access Points**: Weak encryption/default passwords.
* **Core Router**: Compromise here = full control.

**Recommended Countermeasures (Cost-Conscious):**

* Implement strict ACLs between VLANs.
* Enable MAC address filtering on Wi-Fi.
* Enforce strong password policy and remove defaults.
* Add isolated VLAN for IoT/guest devices.
* Deploy IDS/IPS for anomaly detection.

**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.

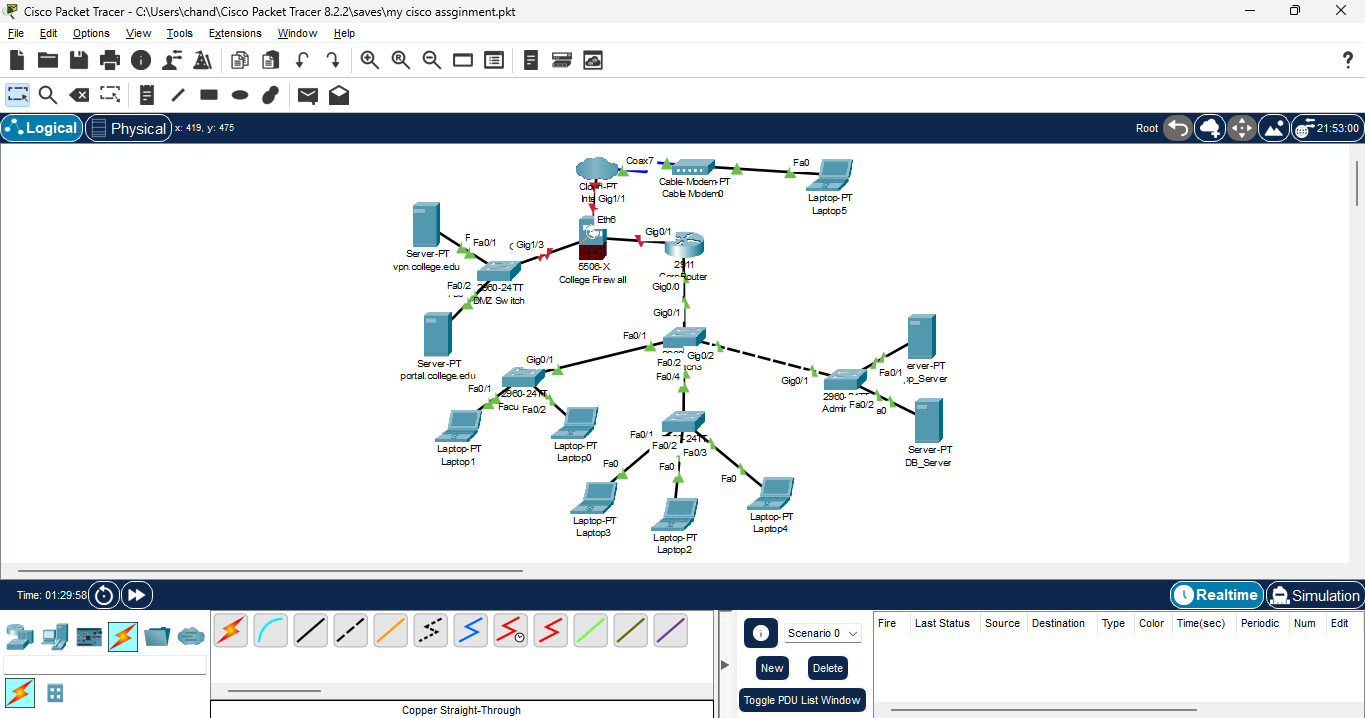
● Justify your architecture with risks, use cases, and fallback strategies.   
  
Deliverables:

● Updated network diagram with new hybrid access components.

● Technical documentation explaining chosen solutions, technologies, risks, and advantages

**Part 2: Secure Hybrid Access Design**

**2.1 Updated Network Diagram with Hybrid Access Components**

****

***(Packet Tracer file showing the Firewall, DMZ with vpn.college.edu and portal.college.edu servers, and remote user)***

**2.2 Technical Documentation**

**Chosen Solutions & Technologies:**

* **Faculty Remote Access:** SSL VPN (vpn.college.edu) in DMZ. Faculty authenticate with credentials and MFA → secure encrypted tunnel → internal resources.
* **Student Remote Access:** Identity-Aware Reverse Proxy (portal.college.edu) in DMZ → provides controlled access to LMS and lab tools.
* **Segmentation:** DMZ isolated from internal servers. Firewall allows only necessary communication.

**Justification of Architecture:**

* **Security:** Internal services never directly exposed.
* **Simplicity:** Single firewall appliance manages VPN, DMZ, and policies.
* **Scalability:** More VPN licenses/proxy capacity can be added easily.

**Risks & Fallback Strategies:**

* VPN server outage → fallback: critical faculty access via proxy with strict MFA.
* Firewall bottleneck → backup router/firewall recommended long term.

**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.

**Part 3: Web Filtering & Policy Enforcement**

**3.1 Final Updated Topology with Filtering Appliance**

**A computer screen shot of a diagram

AI-generated content may be incorrect.**

***(Packet Tracer file showing the dns-filter.college.edu server between the firewall and internal network)***

**3.2 Web Access Policy Document**

**Policy Intent:**  
Ensure responsible usage of resources, prevent misuse, and protect from malicious domains while respecting academic freedom.

**Enforcement Logic:**  
DNS-based filtering chosen for its simplicity, cost-effectiveness, and minimal device overhead.

|  |  |  |  |
| --- | --- | --- | --- |
| **User Role** | **Time** | **Content Category** | **Action** |
| All Users | Always | Malware, Phishing, Illegal Content | **BLOCK** |
| Students | 8:00 AM – 6:00 PM (Mon-Fri) | Social Media, Streaming, Games | **BLOCK** |
| Students | Evenings & Weekends | Social Media, Streaming | **ALLOW** |
| Students | Always | Torrents, P2P File Sharing | **BLOCK** |
| Faculty | Always | All Categories | **ALLOW (Monitor)** |
| Guests | Always | Only Web Browsing | **ALLOW (Restricted)** |

**Logging and Alerting:**

* All filtering events logged to **syslog.college.edu**.
* Repeated blocked attempts trigger alerts.
* IT generates monthly usage and violation reports.

**Additional Enhancements**

* **Compliance & Frameworks:** Architecture aligns with NIST Cybersecurity Framework and Cisco SAFE principles, ensuring industry-standard resilience.
* **Performance:** QoS rules on the firewall prioritize LMS and VoIP traffic over non-essential apps.
* **Incident Response:** A simple playbook should define actions for alerts (e.g., VPN anomalies, repeated policy violations).
* **User Awareness:** Periodic cybersecurity workshops strengthen the “human firewall.”
* **Future Vision:** Migration to a cloud-based **SASE solution** could add Zero Trust, CASB integration, and advanced monitoring.

**Conclusion**

This project implemented a **three-part security enhancement roadmap** for the college:

1. **Audit & Risk Identification** – Mapped weaknesses, highlighted attack surface, and suggested low-cost countermeasures.
2. **Hybrid Access Architecture** – Enabled secure VPN/proxy-based remote access while protecting critical servers inside a DMZ.
3. **Web Filtering Policies** – Enforced responsible internet use with DNS filtering, role-based restrictions, and monitoring.

By combining strong perimeter defences, controlled hybrid access, and adaptive web usage policies, this design transforms the college network into a **secure, resilient, and future-ready environment**. It balances academic freedom with robust cybersecurity, all while remaining practical for limited budgets and IT staff.

**Prepared by:**  
**Saichandana Nunna**