DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
CATEGORY - 1 UNIVERSITY BY UGC
Accredited “A++” by NAAC I Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119

CISCO AICTE Virtual Internship Program 2025

A CISCO AICTE Virtual Internship project report on Cyber Security submitted in partial fulfillment of the requirements for the AICTE-CISCO virtual Internship in Cyber Security Program 2025

SUBMITTED BY: SOHAIL WAJID

AICTE Internship Student Registration ID	**:**	STU682b811f06df41747681567
Registration Number	**:**	43733124
Email	**:**	sohailwajid4618@gmail.com

PART 1

- Analyze your existing university/college campus network topology.
- Map it out the using Cisco Packet Tracer and identify the security controls that are in place today.
- Consider and note how network segmentation is done.
- Observe what kind of intrusion detection systems, firewalls, authentication and authorization systems are in place.
- Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping.
- Aim to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

TASKS

1. **Campus Network Analysis:** conduct an analysis of your college campus network topology, including the layout, devices, and connections.

2. **Network Mapping:** Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and other relevant network components.

3. **Attack Surface Mapping:** Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design. Consider factors such as unauthorized access, data breaches, and network availability.

DELIVERABLES

1. Network topology diagram depicting the existing infrastructure and attack surface findings.

2. Security assessment report highlighting identified security risks, proposed solutions and countermeasures to mitigate attack surface risks.

SOLUTION

1. **Network Layout**

Imagine our campus as a bustling town with different districts:

- **Buildings (LANs):** Each building hosts classrooms, labs, and offices.
- **Devices:** Let's meet our network citizens:
- **Routers:** Wise traffic managers directing data between neighborhoods.
- **Switches:** Efficient mail carriers ensuring messages reach the right rooms
- **Access Points:** Friendly Wi-Fi providers connecting everyone.
- **Firewalls:** Vigilant guards at the gates.
- **Servers:** Busy multitasker handling web, email, databases, and backups.
- **Computers:** Students and faculty each with their own desks.
- **Connections:** High-speed cables link them all.

2. **Network Mapping with Cisco Packet Tracer:**

- **Routers:** Central hubs connecting different buildings.
- **Switches:** They ensure messages find their way.
- **Firewalls:** Guards checking who enters.
- **Intrusion Detection Systems (IDS):** Our alert watchdogs.
- **Authentication s Authorization:** Keys and permissions—only the right folks get in.

3. **Attack Surface Mapping:** Our treasure hunt for vulnerabilities:

- **Unauthorized Access:** Hidden trapdoors (let's seal them).
- **Data Breaches:** Protect sensitive information .
- **Network Availability:** Keep the drawbridge up.

PROSED SOLUTIONS

1. **Technological Upgrades**
    - **Patch Management:** Imagine our wizards constantly updating magical spells our network devices need the same care. Keep routers, switches, and servers patched with the latest security updates.
    - **Password Enchantment:** Cast a strict password policy spell. Complex passwords (a mix of letters, numbers, and special symbols) are our shields.
    - **Multi-Factor Authentication (MFA):** Extra layers of protection—like adding secret runes to the castle gates.
2. **Wireless Warding:**
    - Upgrade our Wi-Fi enchantments to WPA3—no more outdated magic circles.
    - Regularly inspect and ward off legacy wireless artifacts—they might harbor ancient curses.
3. **Intrusion Detection s Prevention Spells (IDPS):**
    - Deploy magical IDS/IPS guardians and they sense both known and mysterious threats.
    - Keep their spellbooks up-to-date—like sharpening magical swords.
    - Network anomalies.

3. **Firewall Incantations:**
    - Review and fine-tune firewall spells—close unnecessary portals which is an open port.
    - Segment wisely—critical network segments.

4. **Procedural Enchantments:**

- **Security Audits:** Annual castle inspections by third-party knights—uncover hidden passages.
- **Penetration Testing Quests:** Simulate attacks—find weak spots before real dragons do.
- **Security Training Scrolls:** Teach everyone to recognize suspicious runs.

5. **Incident Response Magic Circle:**

- Create a magical playbook—clear steps for handling cyber threats.
- Practice mock battles—so every knight knows their role during an attack.

6. **Physical Barrier Spells:**

- Server rooms with surveillance crystals and enchanted locks.
- Keep out unwelcome intruders with only authorized wizards allowed!

CONCLUSION

- Implementing the recommended solutions and countermeasures into practice is crucial to protecting our university's network from potential cyber attacks. With digital threats becoming more advanced and frequent, it is necessary to strengthen our security systems and update our policies proactively. Doing so will safeguard both academic resources and the personal information of students and staff, helping to preserve the institution's credibility and trustworthiness.
- By following these measures, we will build stronger defences and keep our network well-prepared against future threats. This dedication to cyber security will provide a safe and dependable digital environment for teaching, learning, and research, ensuring the continued success and positive reputation of our university.

PART 2

- Your college has hired you to design and architect a hybrid working environment for its faculty and students.
- Faculty members will be provided with laptops by the college to connect to the college network and access faculty specific services C resources.
- These should be accessible from home as well as on campus.
- Students are allowed to connect using their personal devices to access student specific services C resources from home as well as on campus. Campus network services should not be exposed to public internet and accessible only via restricted networks.

TASKS

1. Design network segmentation based on user roles (faculty vs. students).
2. Recommend secure access tools.
3. Define trust models, authentication flows, and access control mechanisms for internal applications.
4. Update the campus network topology to include remote access pathways, gateways, and policy enforcement zones.
5. Justify the proposed architecture by analyzing risks, use cases, and strategies.

DELIVERABLES

1. Updated network diagram with new hybrid access
2. Technical documentation explaining chosen solutions, technologies, risks, and advantages.

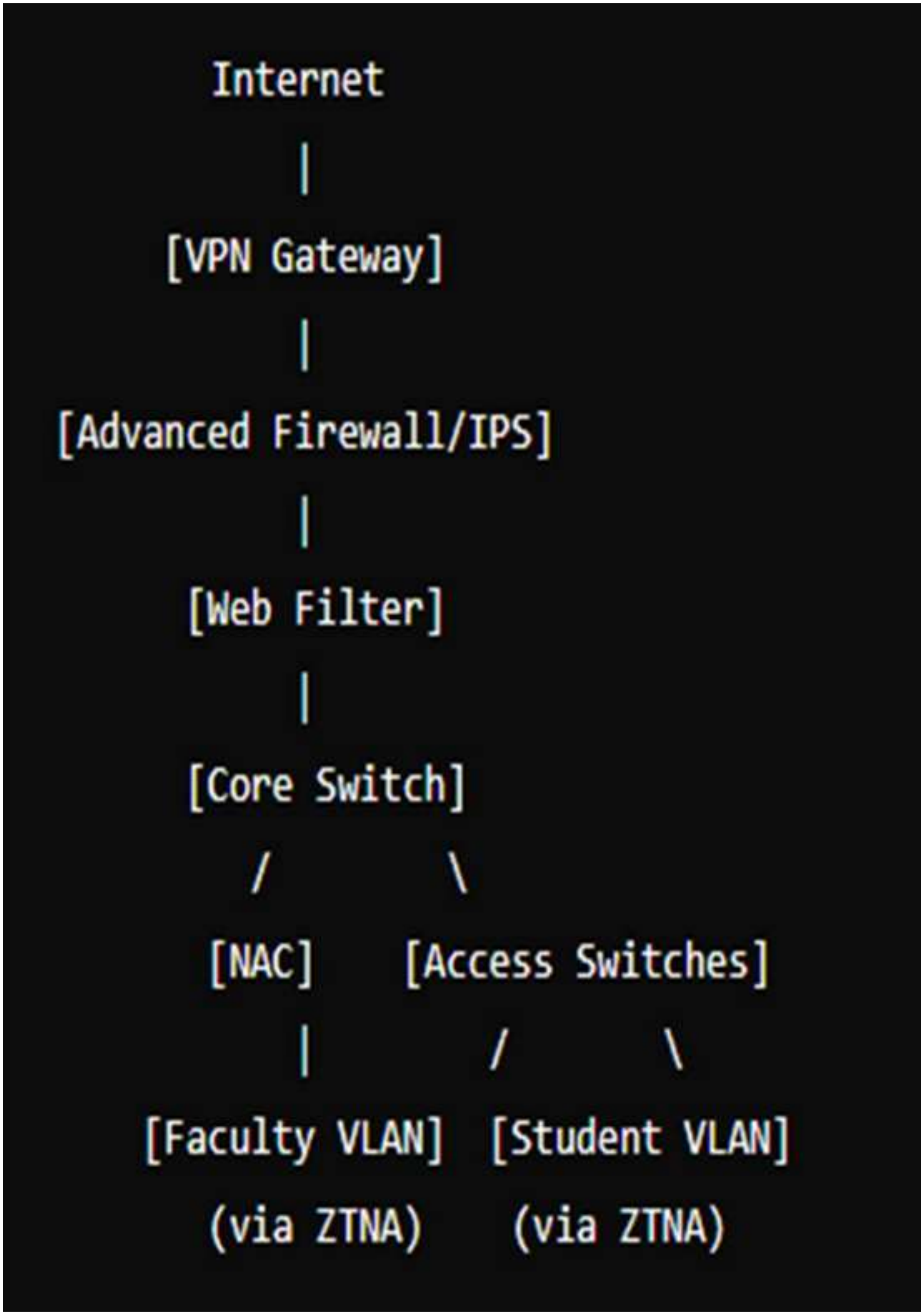
SOULTION

TASK 1: Options for Achieving a Secure Hybrid Working Environment

1. **Remote Access for Faculty**: Faculty members need secure access to campus resources from both home and on campus.
2. **Access for Students**: Students need secure access to student-specific services from personal devices, both at home and on campus.
3. **Network Security**: Campus network services should be restricted to authorized users and not exposed to the public internet.
4. **Virtual Private Network (VPN)**:
   - **For Faculty**: A VPN can provide secure remote access to campus resources. Each faculty member's laptop can be configured with VPN client software.
   - **For Students**: A separate VPN profile can be provided to students for secure access to student-specific resources.
5. **Zero Trust Network Access** :
   - **For Faculty and Students**: ZTNA ensures that every access request is authenticated, authorized, and encrypted. It is particularly useful for securing remote access to sensitive resources.
6. **Network Access Control (NAC)**:
   - **For On-Campus Security**: NAC solutions can enforce security policies on devices before they are allowed to connect to the network. This ensures that only compliant devices can access the network.
7. **Multi-Factor Authentication (MFA)**:
   - **For Enhanced Security**: MFA adds an additional layer of security for accessing resources, requiring a second form of verification beyond just a password.
8. **Firewalls and Intrusion Prevention Systems (IPS)**:
   - **For Network Protection**: Implementing advanced firewalls and IPS can help protect the network from external threats and unauthorized access.
9. **Segmentation and VLANs**:

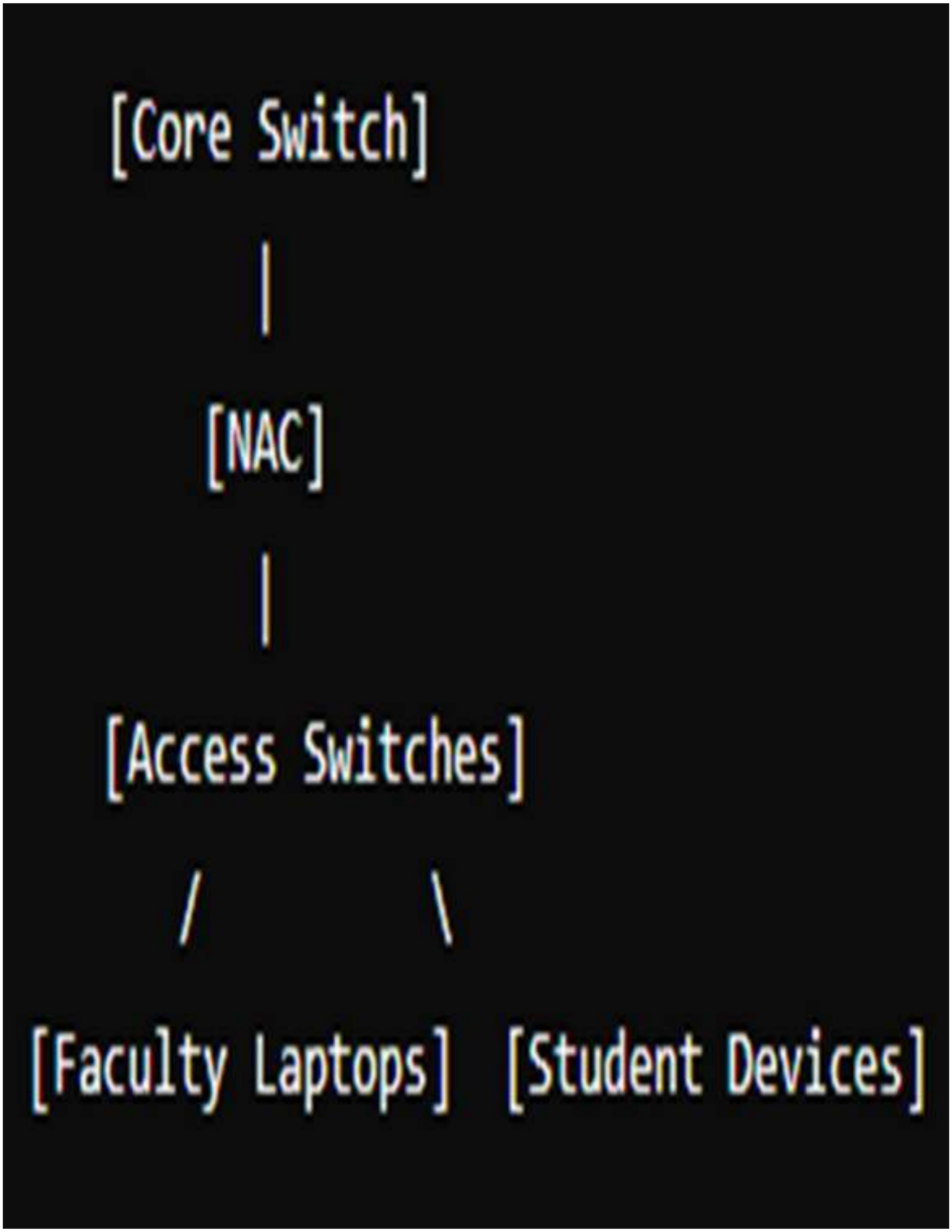
   - **For Network Isolation**: Segmentation and the use of VLANs can isolate different parts of the network, ensuring that faculty and student resources are kept separate.

TOPOLOGY DIAGRAM



```
          Internet
              |
        [VPN Gateway]
              |
   [Advanced Firewall/IPS]
              |
         [Web Filter]
              |
        [Core Switch]
           /        \
        [NAC]    [Access Switches]
          |          /        \
   [Faculty VLAN]  [Student VLAN]
     (via ZTNA)     (via ZTNA)
```

TOPOLOGY DIAGRAM



```
   [Core Switch]
         |
      [NAC]
         |
   [Access Switches]
      /         \
[Faculty Laptops]  [Student Devices]
```

TASK 3: RISKS AND ADVANTAGES

RISKS

- **Complexity**: Implementing and managing a comprehensive security solution can be complex and require specialized knowledge.
- **Performance**: VPNs and ZTNA solutions can introduce latency, which might affect user experience.
- **Cost**: Advanced security solutions can be expensive to deploy and maintain.

ADVATANGES

- **Enhanced Security**: Strong access controls and network segmentation greatly reduce the risk of unauthorized access and data breaches.
- **Flexibility**: Faculty and students can securely access resources from both home and on campus.
- **Compliance**: Ensures compliance with data protection regulations by securing access to sensitive resources.

CONCLUSION

- By implementing VPN gateways, advanced firewalls/IPS, core switches with VLAN segmentation, and Zero Trust/Network Access Control policies, the institution can build a secure hybrid working environment for both faculty and students. These measures ensure authenticated, role-based access, safeguard sensitive resources, and provide layered defense against potential threats. Ultimately, this architecture not only enhances data security but also supports flexible and reliable academic operation.

PART 3

- The college has discovered that students are misusing campus resources and accessing irrelevant sites. They want a solution which will restrict access to only allowed categories of web content.

TASKS & DELIVERABLES

1. Explore how this can be achieved and what kind of network security product can provide this capability.
2. Update the campus network topology with new component.
3. Explain the reasoning behind your choice, detailing the risks C advantages of your proposed solution.
4. Write the policies you would apply.
5. Update the campus network topology with new component.
6. Explain the reasoning behind your choice, detailing the risks advantages of your proposed solution.

SOLUTION

- To address the issue of students misusing campus resources and accessing irrelevant sites, the college can implement a web content filtering solution. This can be achieved by using network security products that provide content filtering capabilities. Here are the tasks and deliverables for this solution.

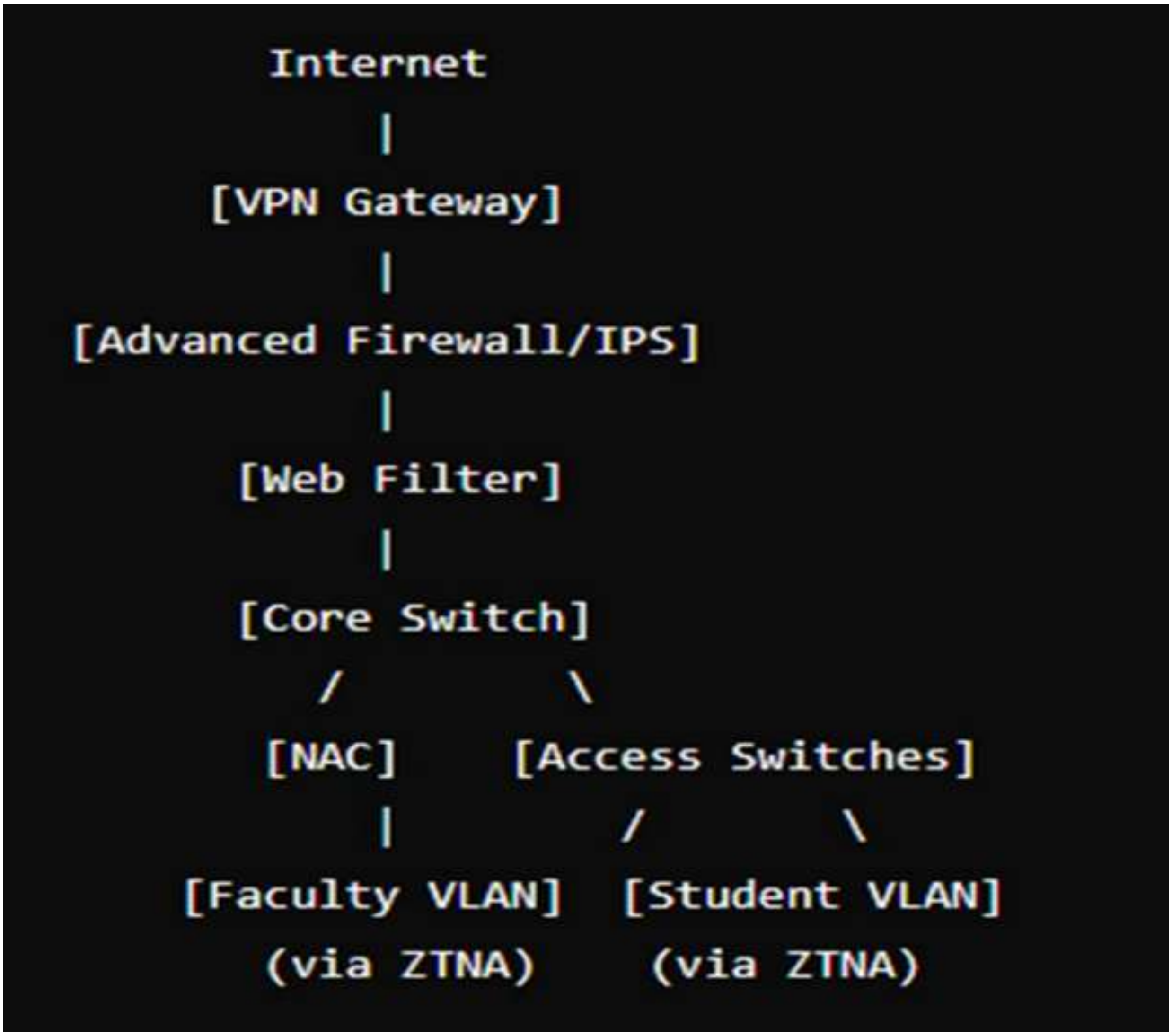
1. Explore Network Security Products for Web Content Filtering

Several network security products offer web content filtering capabilities, including:

- **Cisco Umbrella**: A cloud-based security platform that provides DNS-layer security, web content filtering, and threat intelligence.
- **Palo Alto Networks Next-Generation Firewall**: Provides advanced security features, including web content filtering.
- **Sophos XG Firewall**: Offers web filtering, application control, and other security features.
- **Barracuda Web Security Gateway**: A dedicated appliance for web filtering and protection.

2. Update the Campus Network Topology with New Components

Here's an updated network topology diagram including a web content filtering component:

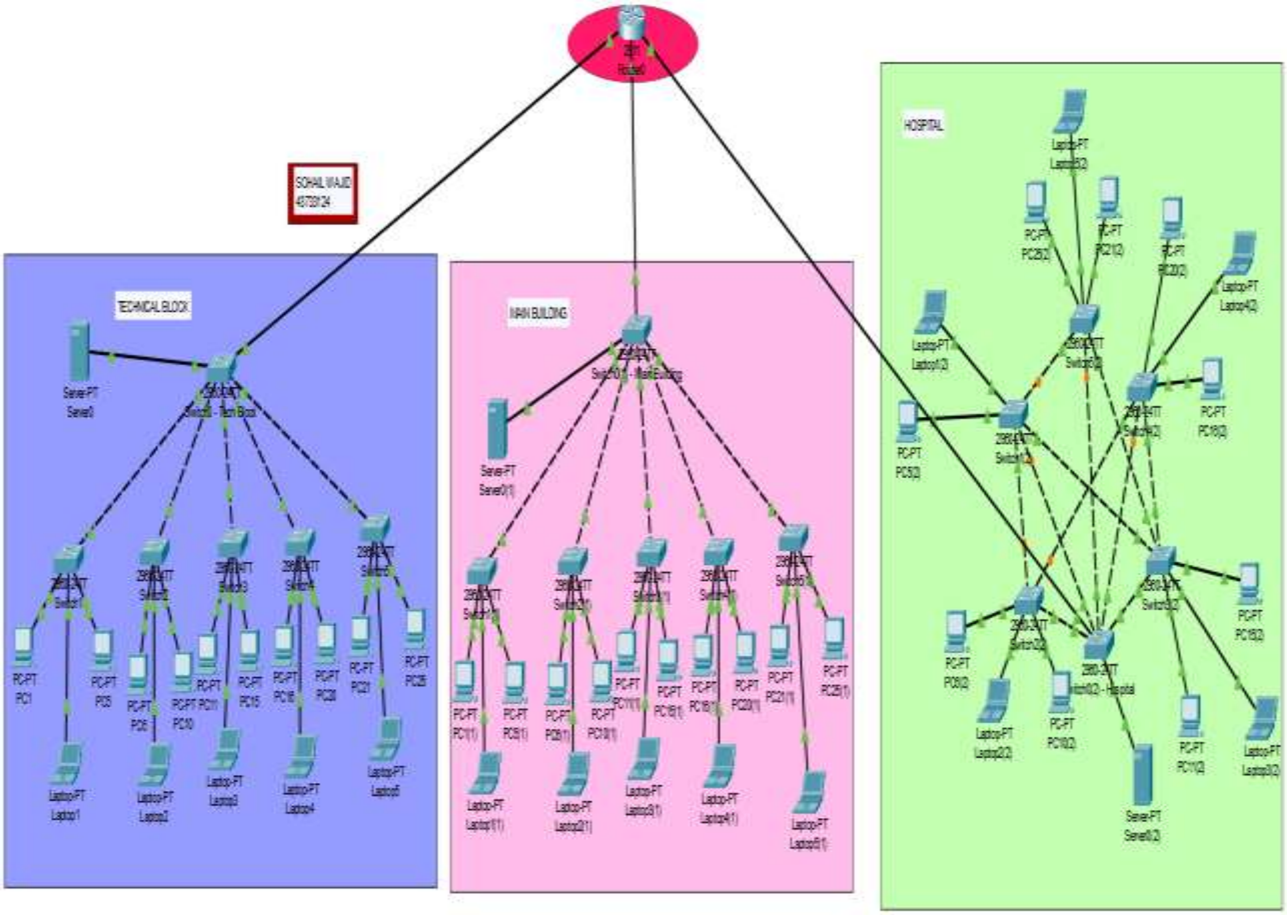


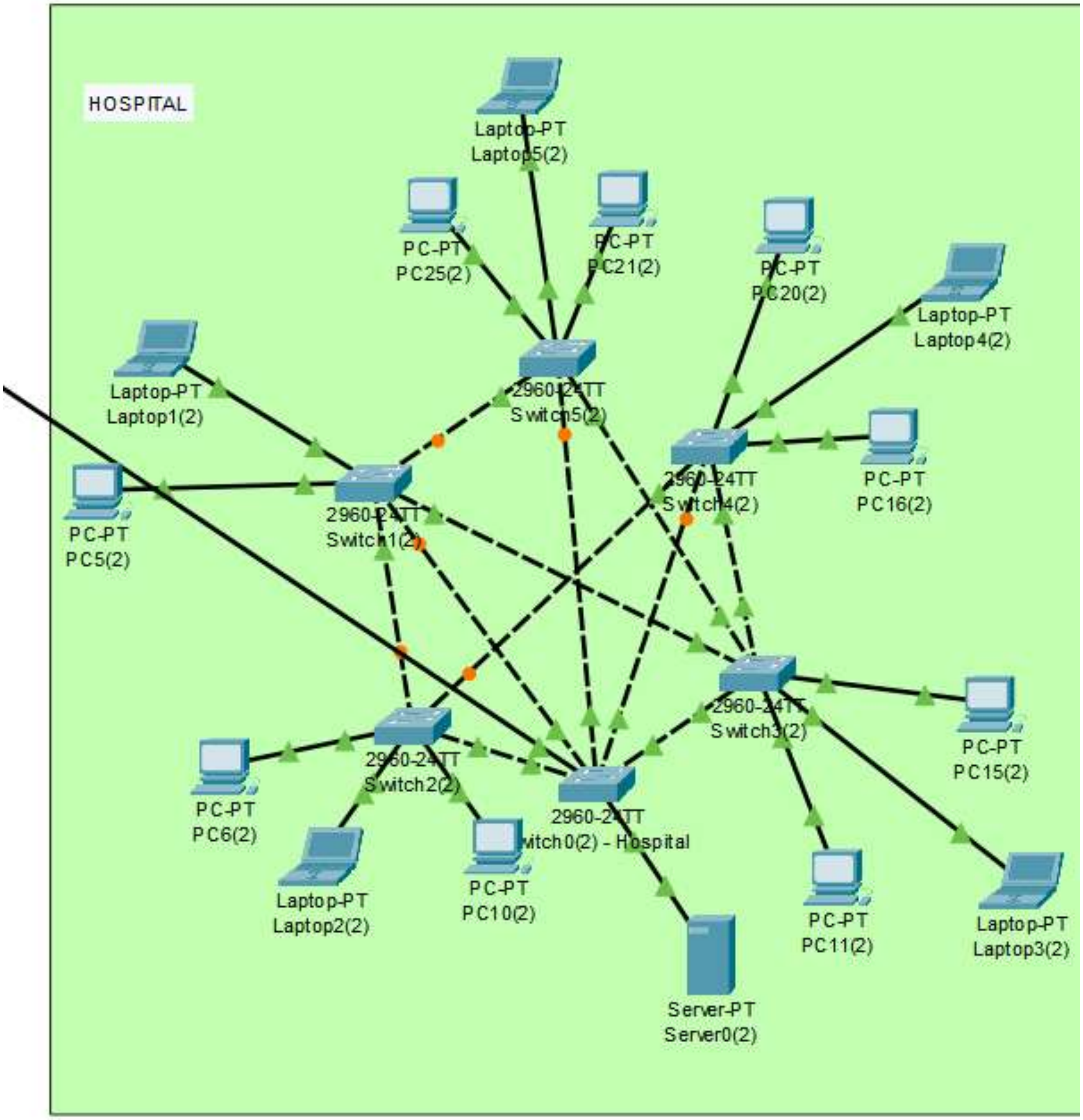
```
         Internet
             |
       [VPN Gateway]
             |
  [Advanced Firewall/IPS]
             |
        [Web Filter]
             |
        [Core Switch]
           /        \
        [NAC]    [Access Switches]
             |         /        \
     [Faculty VLAN]  [Student VLAN]
        (via ZTNA)    (via ZTNA)
```

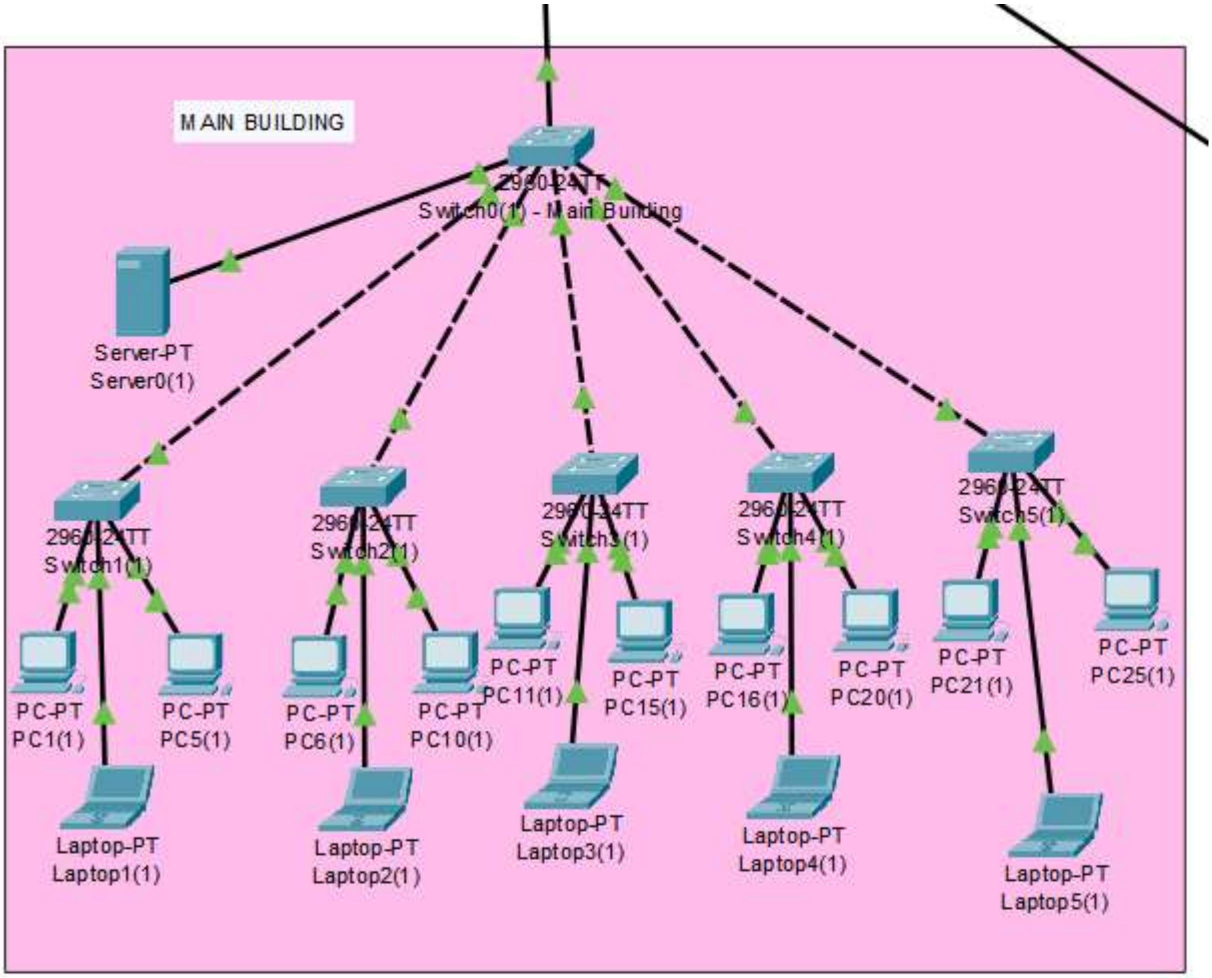
3. Explain the Reasoning Behind the Choice:

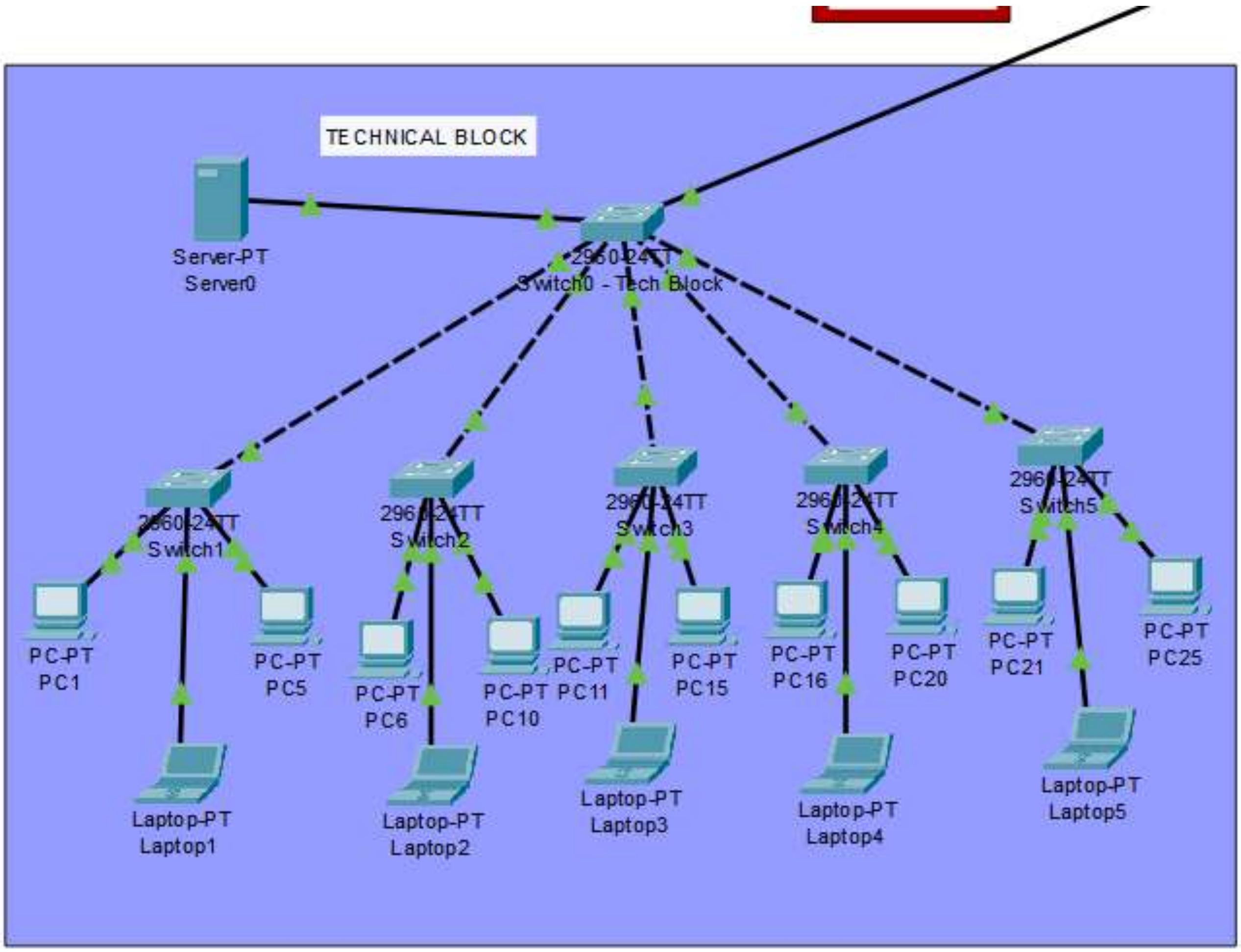
- **Scalability**: Suitable for both small and large networks, making it adaptable as the college's network grows.
- **Ease of Management**: Centralized management and reporting capabilities simplify administration.
- **Performance**: Devices are known for their high performance and low latency, ensuring that the network remains responsive.
- **Integration**: Integrates well with existing network components like the NAC and core switches.

Proposed Architecture Diagram: https://github.com/Sohailwajid23/CISCO-CYBERSECURITY




HOSPITAL
Laptop-PT
Laptop5(2)
PC-PT
PC25(2)
PC-PT
PC21(2)
PC-PT
PC20(2)
Laptop-PT
Laptop4(2)
Laptop-PT
Laptop1(2)
2960-24TT
Switch5(2)
2960-24TT
Switch4(2)
PC-PT
PC16(2)
PC-PT
PC5(2)
2960-24TT
Switch1(2)
2960-24TT
Switch3(2)
PC-PT
PC15(2)
2960-24TT
Switch2(2)
PC-PT
PC6(2)
2960-24TT
witch0(2) - Hospital
Laptop-PT
Laptop2(2)
PC-PT
PC10(2)
PC-PT
PC11(2)
Laptop-PT
Laptop3(2)
Server-PT
Server0(2)


MAIN BUILDING
2960-24TT
Switch0(1) - Main Building
Server-PT
Server0(1)
2960-24TT
Switch1(1)
2960-24TT
Switch2(1)
2960-24TT
Switch3(1)
2960-24TT
Switch4(1)
2960-24TT
Switch5(1)
PC-PT
PC1(1)
PC-PT
PC5(1)
PC-PT
PC6(1)
PC-PT
PC10(1)
PC-PT
PC11(1)
PC-PT
PC15(1)
PC-PT
PC16(1)
PC-PT
PC20(1)
PC-PT
PC21(1)
PC-PT
PC25(1)
Laptop-PT
Laptop1(1)
Laptop-PT
Laptop2(1)
Laptop-PT
Laptop3(1)
Laptop-PT
Laptop4(1)
Laptop-PT
Laptop5(1)


TECHNICAL BLOCK
Server-PT
Server0
2960-24TT
Switch0 - Tech Block
2960-24TT
Switch1
2960-24TT
Switch2
2960-24TT
Switch3
2960-24TT
Switch4
2960-24TT
Switch5
PC-PT
PC1
PC-PT
PC5
PC-PT
PC6
PC-PT
PC10
PC-PT
PC11
PC-PT
PC15
PC-PT
PC16
PC-PT
PC20
PC-PT
PC21
PC-PT
PC25
Laptop-PT
Laptop1
Laptop-PT
Laptop2
Laptop-PT
Laptop3
Laptop-PT
Laptop4
Laptop-PT
Laptop5