

**DEPARTMENT OF CSEAI**

# **KIET Groups of Institutions**

**Accredited “A++” by NAAC | Approved by AICTE  
Delhi Meerut Road, Muradnagar, Uttar Pradesh**

## **Cisco AICTE Virtual Internship Program 2024**

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 2024

Submitted By : AASTHA JAIN

**AICTE ID :** STU63e8c0f3e010e1676198131

**Student ID :** 2100291520002

**Email:** [aastha.2125csai1002@kiet.edu](mailto:aastha.2125csai1002@kiet.edu)

# Cyber Shield: Defending the network

## Problem Statement:

### PART 1:

Analyse 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:

The query is unclear. However, based on the provided sources, it appears you are asking for a discussion on the topic of network attack surface mapping and its relevance to campus network design using Cisco Packet Tracer. Here is a detailed response:

### Network Attack Surface Mapping :

Mapping the attack surface of a network involves identifying and assessing potential avenues through which an attacker could exploit vulnerabilities to compromise the security or integrity of the network. A comprehensive attack surface mapping exercise involves reviewing network topology, identifying potential weaknesses, and proposing countermeasures to mitigate these risks.

## Campus Network Analysis

Attached Aasthajain02 [[GitHub Link](#)] file Where I have made the Network Mapping of KIET Groups of institutions Ghaziabad Using Cisco Packet tracer

### 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.
  - **Computers:** Students and faculty—each with their own desks.
  - **Servers:** Busy multitaskers handling web, email, databases, and backups.
  - **Connections:** High-speed cables (like secret tunnels) link them all.

### Network Segmentation

Network segmentation is a key security control that involves dividing a network into smaller, isolated segments to limit the spread of a potential attack. This can be achieved through the use of VLANs (Virtual Local Area Networks), subnets, and access control lists (ACLs). By segmenting the network, administrators can restrict access to sensitive areas of the network and reduce the attack surface.

### Intrusion Detection & Prevention Spells (IDPS):

- Deploy magical IDS/IPS guardians—they sense both known and mysterious threats.
- Keep their spell books (signatures) up-to-date—like sharpening magical swords.
- Watch for unusual energy fluctuations (network anomalies).

### Authentication and Authorization Systems

Authentication and authorization systems are critical for ensuring that only authorized users have access to network resources. These systems verify the identity of users and devices and grant access based on predefined policies. In a campus network design, authentication and authorization systems should be integrated with other security controls to ensure seamless and secure network resources.

## Attack Surface Mapping

- **Identify Entry Points:** Consider potential vulnerabilities and entry points for cyber-attacks:
  - **External Entry Points:** Internet-facing devices (firewalls, web servers).
  - **Internal Entry Points:** Weaknesses in segmentation (misconfigurations allowing lateral movement).
  - **User Access Points:** Vulnerabilities in authentication mechanisms or phishing attacks targeting users.
- **Data Breach Risks:** Evaluate risks related to sensitive data (student records, financial information) and how they are protected.
- **Service Availability:** Assess risks to network availability from denial-of-service (DoS) attacks or infrastructure failures.
- **Propose Countermeasures:** Based on the findings, propose countermeasures to mitigate the identified risks, such as implementing firewalls, IDS systems, and network segmentation

## Countermeasures

Some countermeasures that can be proposed to mitigate the identified risks include:

- 1. Implementing Network Segmentation:** Divide the network into smaller, isolated segments to limit the spread of a potential attack.
- 2. Configuring Firewalls and IDS systems:** Strategically place firewalls and IDS systems to detect and prevent unauthorized access to the network.
- 3. Implementing Strong Authentication and Authorization:** Integrate authentication and authorization systems with other security controls to ensure seamless and secure access to network resources.
- 4. Conducting Regular Security Audits:** Regularly conduct security audits to identify and address potential vulnerabilities before they can be exploited.

## Conclusion:

The implementation of these proposed solutions and countermeasures is crucial for safeguarding our university's network against potential cyber threats. As digital threats continue to evolve in complexity and severity, the proactive enhancement of our network's security infrastructure and policies is not merely beneficial but essential. These measures will

not only protect sensitive academic data but also safeguard the personal information of our students and staff, thereby maintaining the trust and integrity of our institution. Adopting these recommendations will fortify our defenses and ensure that our network remains resilient against cyber threats, supporting our ongoing commitment to providing a secure and reliable digital environment for all educational activities.

## **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 & 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 & resources from home as well as on campus. Campus network services should not be exposed to the public internet and accessible only via restricted networks.

### **Tasks & Deliverables:**

1. Explore options for how to achieve this and what kind of network security product can provide this capability
2. Update the campus network topology with the new components
3. Explain the reasoning behind your choices detailing the risks & advantages of your proposed solution

### **Solution:**

The college has hired me to design and architect a hybrid working environment for its faculty and students. This environment will enable faculty members to access college resources and services from both home and on campus using college-provided laptops, while students will use their personal devices to access student-specific services and resources from both home and on campus. The campus network services should not be exposed to the public internet and should only be accessible via restricted networks

## **Explore Options for Network Security Products:**

### **Products and Technologies:**

#### **1. Virtual Private Network (VPN):**

- **Product Example:** Cisco AnyConnect Secure Mobility Client
- **Use:** Securely connects faculty and students to the college network from remote locations by encrypting traffic and using strong authentication methods.

#### **2. Network Access Control (NAC):**

- **Product Example:** Cisco Identity Services Engine (ISE)
- **Use:** Manages and enforces security compliance on all devices that access the network, ensuring that only authorized devices can access specific resources.

### 3. Multi-Factor Authentication (MFA):

- **Product Example:** Duo Security ○ **Use:** Adds an additional layer of security by requiring two or more verification methods to gain access to the network, reducing the risk of unauthorized access.

### 4. Cloud Access Security Broker (CASB):

- **Product Example:** Cisco Cloudlock
- **Use:** Protects data in cloud services and ensures that only authorized users can access sensitive information remotely.

## Updating the Campus Network Topology:

### New Components:

#### 1. VPN Gateways:

- **Placement:** Deployed at the network perimeter to handle incoming VPN connections securely.

#### 2. NAC Solutions:

- **Placement:** Integrated with the network infrastructure to monitor and control access at various network access points.

#### 3. MFA Systems:

- **Integration:** Across all user access points to the network, including initial login portals and cloud-based services access.

### Updated Network Topology Diagram:

The diagram will include the newly added VPN gateways and points of MFA integration, demonstrating the comprehensive approach to securing remote access.

### Risks & Advantages:

#### □ VPN:

- **Risks:** Potential for decreased network performance due to encryption overhead.
- **Advantages:** Provides secure remote access, encrypts data in transit, and effectively extends the network perimeter in a controlled manner.

#### • NAC: ○ **Risks:** Complex configuration and maintenance. ○ **Advantages:**

Ensures that only compliant and authorized devices can connect to the network, significantly reducing the risk of infected devices compromising the network.

#### • MFA: ○ **Risks:** User resistance due to added complexity in the login process.

- **Advantages:** Greatly enhances security by mitigating the risk of compromised passwords leading to unauthorized access.

#### □ CASB:

- **Risks:** Can be resource-intensive in terms of monitoring and managing cloud access.

- **Advantages:** Provides visibility and control over data in the cloud, ensuring compliance and data security across remote access scenarios.

## **Conclusion:**

Implementing these technologies will create a robust hybrid working environment that supports the dynamic needs of faculty and students. It ensures secure and controlled access to network resources from both on-campus and remote locations, while maintaining compliance with security policies and protecting against potential cyber threats. This design not only meets the current needs but is scalable for future expansion and integration with emerging technologies.

## **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(s)
3. Explain the reasoning behind your choice, detailing the risks & advantages of your proposed solution
4. Write the policies you would apply (can use simple English language commands)

## **Solution:**

# **Network Security Solutions for Campus Networks**

## **1. Web Content Filtering Solutions**

- **Product Example: Cisco Umbrella**
- **Use:** Provides DNS-based security by blocking access to websites based on categories, security risks, or specific URLs, ensuring that only approved content is accessible.

## **2. Firewall with Integrated Security Services**

- **Product Example: Cisco Firepower**
- **Use:** Offers capabilities such as URL filtering, malware detection, and intrusion prevention, which can be configured to enforce web access policies.

## Updated Campus Network Topology

### 1. Cisco Umbrella

- **Placement:** Integrated at the DNS layer to filter internet traffic and prevent access to non-approved websites before a connection is even established.

### 2. Cisco Firepower

- **Placement:** Deployed alongside existing firewalls to enhance security with deep packet inspection and real-time threat intelligence.

- **Updated Network Topology Diagram:** The diagram will now include Cisco Umbrella for DNS filtering and Cisco Firepower for enhanced firewall protection, showing their integration points within the existing network infrastructure.

## Risks & Advantages

### 1. Cisco Umbrella

- **Risks:**
  - Overblocking can occur, where legitimate educational sites might be inadvertently blocked if not properly categorized.
- **Advantages:**
  - Provides a first line of defense at the DNS layer, effectively preventing access to unwanted sites quickly and efficiently.

### 2. Cisco Firepower

- **Risks:**
  - May require significant resources to manage and maintain, especially with frequent updates and policy changes.
- **Advantages:**
  - Offers comprehensive network protection beyond URL filtering, including threat detection and response capabilities.

## Sample Policies for Web Content Filtering

1. **Block Access to Non-Educational Entertainment Sites:**
  - Deny access to categories "Entertainment, Gaming, Social Media" during school hours.
2. **Allow Educational and Research-Related Websites:**
  - Allow access to categories "Education, Research" at all times.
3. **Restrict Certain High-Bandwidth Activities:**
  - Deny access to categories "Streaming Media, File Sharing" except during nonschool hours.
4. **Custom Rules for Specific Needs:**
  - Allow access to "youtube.com/edu" for educational videos; deny "youtube.com/watch."
  - Block websites categorized under "Adult Content, Gambling" at all times.



## Conclusions

The deployment of Cisco Umbrella alongside Cisco Firepower will enable the college to effectively manage and monitor web traffic. This ensures that only content relevant to educational and research activities is accessible. By implementing these comprehensive content filtering measures, the college can maintain control over its network usage, prevent misuse, and align technology use with educational goals and policies. It maximizes network resource utilization while fostering a safer and more productive educational environment.

## Cloud Security

### Problem Statement:

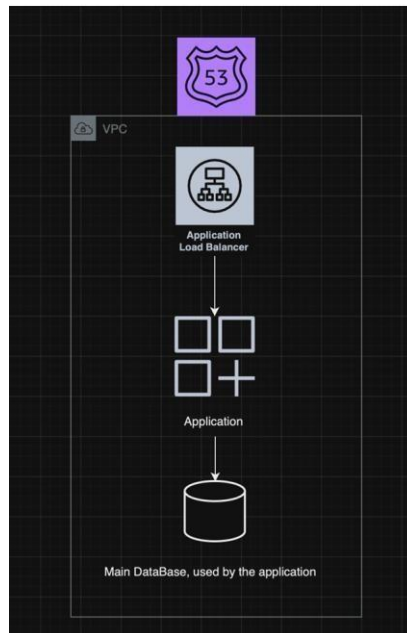
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

Last year during 15Aug sale, the start-up faced two challenges - the service was unable to handle the huge influx of web requests and the company faced flak and complaints on social media. They also experienced a DDOS attack during this time, which made the situation worse.

You have been asked to propose a revised design to address this problem in preparation for the upcoming sale.

Refer the existing simplified architecture diagram

1. The existing architecture is very basic, aim to improve availability of the system
2. The existing data base is a bottle neck and is prone to corruption, aim to have backup service available within few seconds
3. During flash sale, the service should be able to handle burst traffic, but the large resources will not be needed on regular days. Your design should incorporate this requirement.
4. To mitigate any DDOS attack, aim to add a perimeter layer controlling access to the service to mitigate the attack.



### Tasks & Deliverables:

1. Consider how to improve scalability and availability of the system and how to be cost efficient
2. Create a new diagram with proposed design improvements
3. Explain the reasoning behind your choices detailing the risks & advantages of your proposed solution
4. Research how DDOS attacks occur, what kind of attacks exist
5. Describe what type of attacks this application can be vulnerable to and how your solution will make it resilient.

### Solution:

#### Proposed Revise Design

##### 1. Improving System Availability:

- **Load Balancing:** Distributing incoming web traffic across multiple instances using an elastic load balancer ensures high availability and fault tolerance. No single server is overloaded.
- **Auto-Scaling:** Automatically adjusting the number of instances based on demand (e.g., during flash sales) prevents performance bottlenecks.

##### 2. Database Scalability and Reliability:

- **Database Clustering:** A clustered environment with a primary and replica setup ensures high availability. The replica serves read requests and acts as a failover solution.

- **Backup and Recovery:** Real-time data replication to a secondary database and regular snapshots enable quick restoration in case of corruption.

### 3. Handling Burst Traffic Efficiently:

- **Content Delivery Network (CDN):** Deploying a CDN caches static content at edge locations, reducing load times and server load during high traffic periods.
- **Caching Strategies:** Implement Redis or Memcached to serve frequently accessed data without hitting the database repeatedly.

### 4. DDoS Attack Mitigation:

- **Perimeter Layer:** Introduce a Web Application Firewall (WAF) to filter out malicious requests commonly found in DDoS attacks.
- **Rate Limiting:** Apply rate limiting to prevent excessive requests from a single source.
- **Third-Party DDoS Protection Services:** Consider Cloudflare or AWS Shield for advanced mitigation techniques.

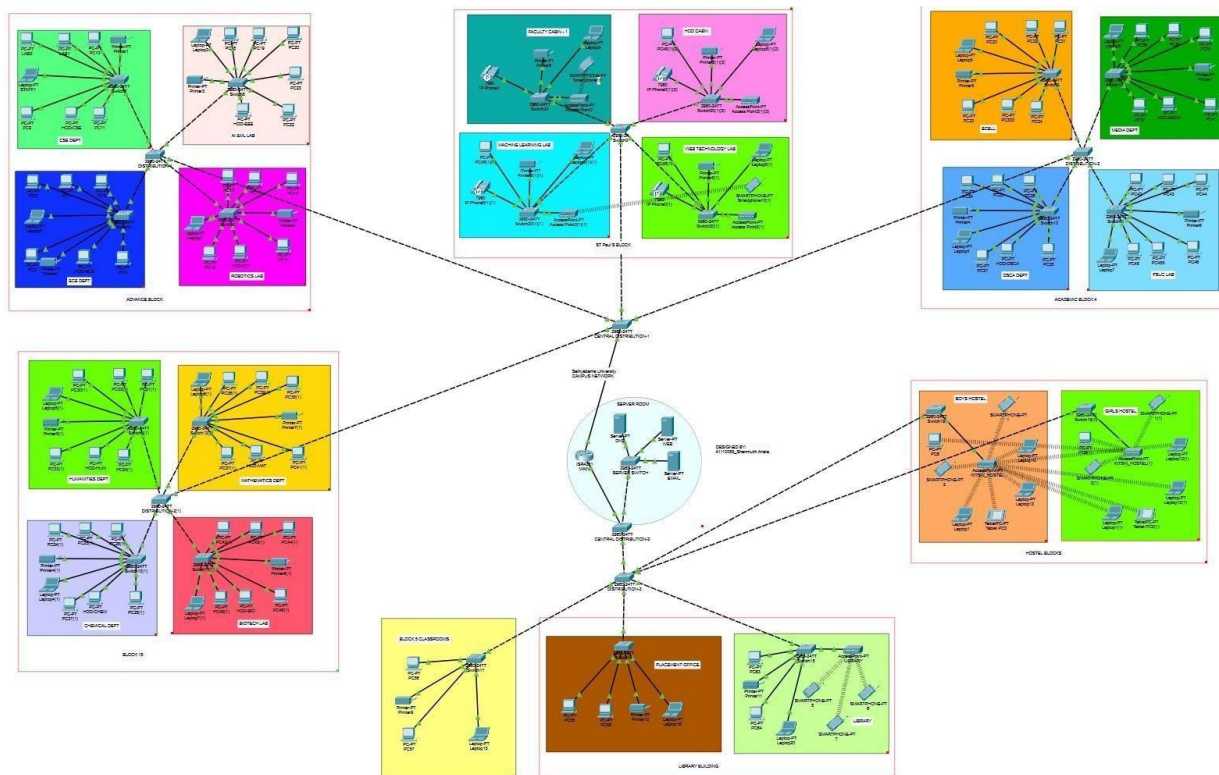
### Updated Cloud Architecture Diagram:

- Load Balancer distributes traffic across web servers.
- Auto-Scaling Group dynamically adjusts resources.
- WAF and DDoS Protection act as the first line of defense.
- Database Cluster (primary and replica) ensures availability.
- CDN and Caching Layers reduce latency during peak traffic.

By implementing these strategies, your startup can achieve resilience, scalability, and security for its e-commerce platform. It's a smart move to address current challenges and prepare for future growth.

-----

## Network Mapping with Cisco Packet Tracer:



Main Server

