Cisco-AICTE Virtual Internship Program 2024

Chandigarh University

Chandigarh University, NH-05, Ludhiana, Highway, Chandigarh State, Punjab 140413

A project report on cybersecurity, submitted in partial fulfilment of the requirements for the AICTE-CISCO Virtual Internship in Cyber Security Program 2024.

Submitted By: BEVARA PRAVEEN

AICTE Internship Student Registration ID: STU64e094e774c0d1692439783

Student ID (Enrolment Number): 21BCS3517

Emai: praveenbevara33@gmail.com

Contact Info: +916301713865

Github Link: https://github.com/Praveen3517-cu/Cisco_VIT_CS_2024

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.

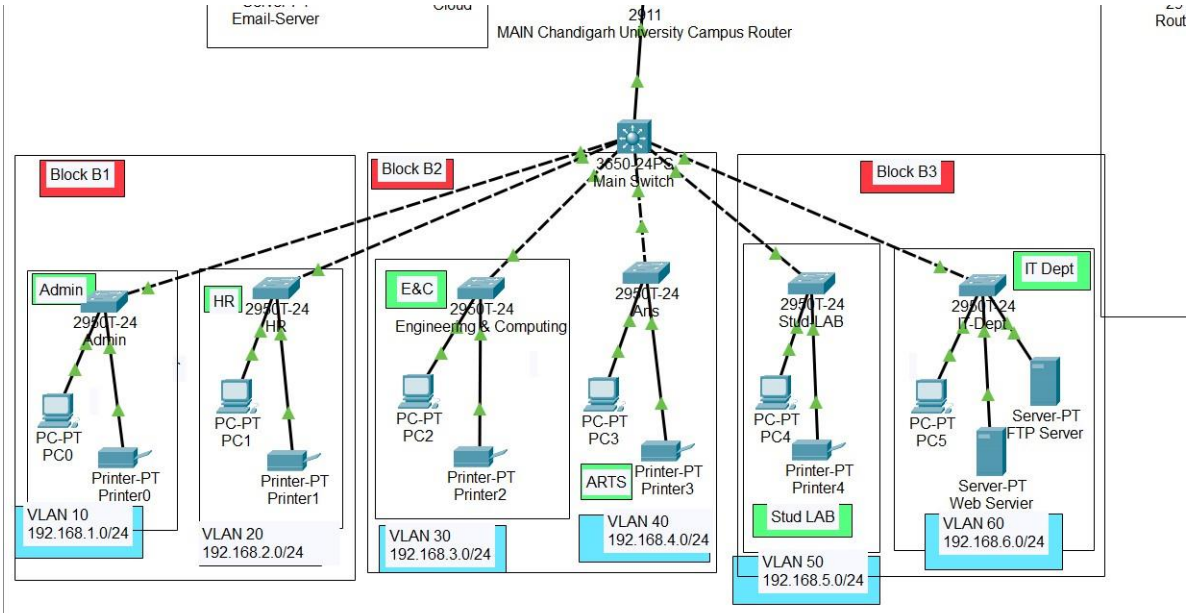
Deliverables:

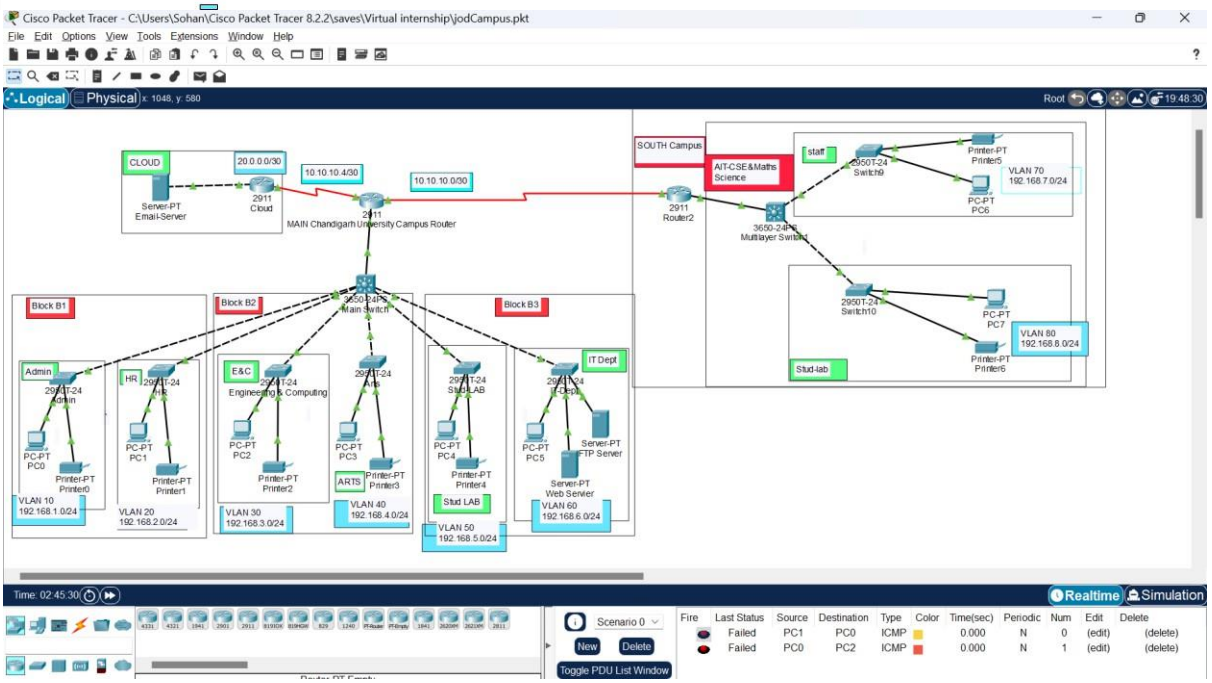
1. Network topology diagram depicting the existing infrastructure and attack surface findings.
2. Security assessment report highlighting identified security risks, proposed solutions and countermeasures to mitigate attack surface risks.

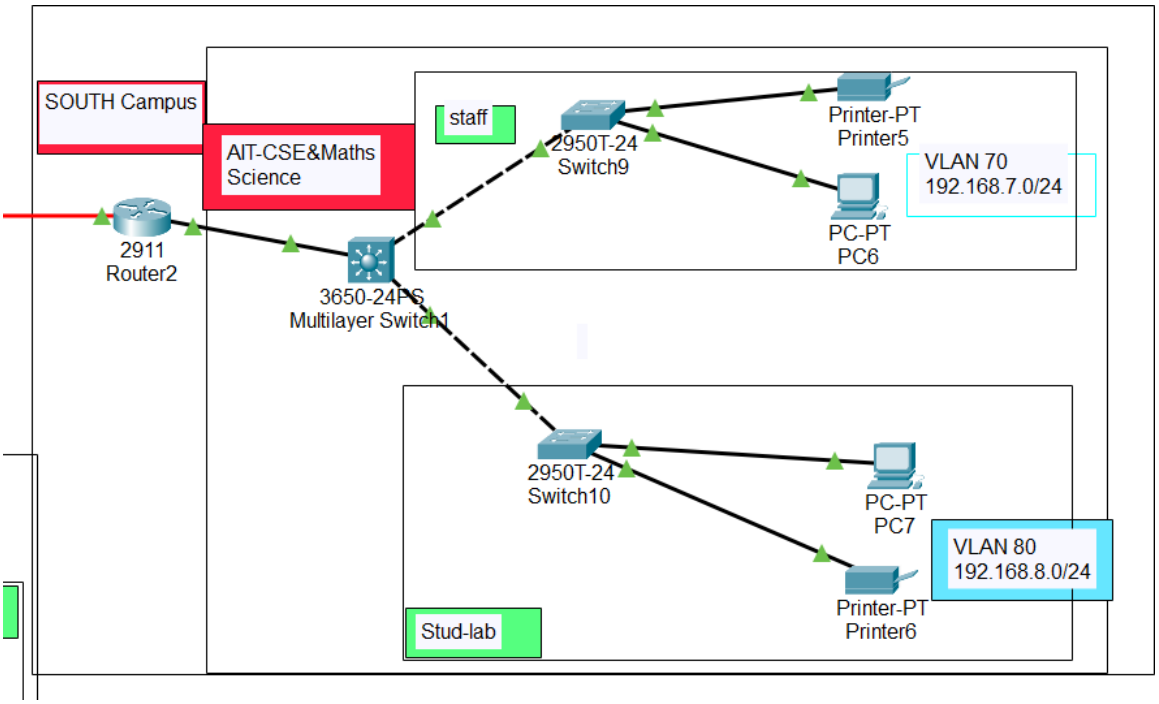
Solution:

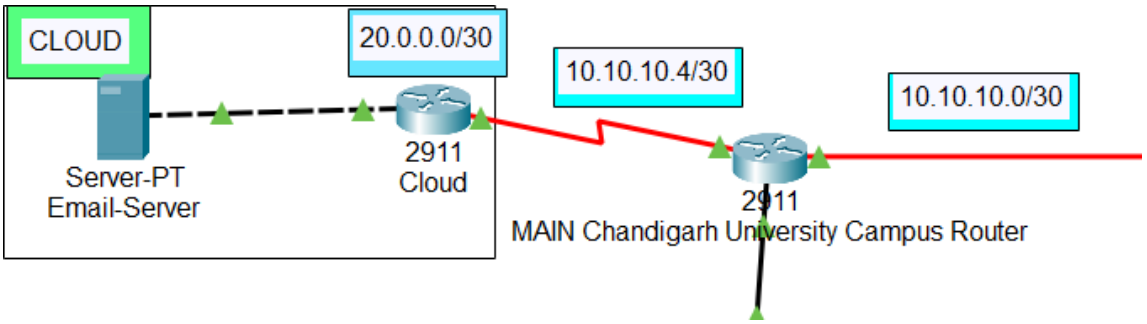
1. Network Topology Diagram

Below is a high-level representation of a typical college campus network topology. Please adapt this to match your actual campus layout.


Email-Server
2911
MAIN Chandigarh University Campus Router
Block B1
Block B2
Block B3
3650-24PS
Main Switch
Admin
2950T-24
Admin
PC-PT
PC0
Printer-PT
Printer0
VLAN 10
192.168.1.0/24
HR
2950T-24
HR
PC-PT
PC1
Printer-PT
Printer1
VLAN 20
192.168.2.0/24
E&C
2950T-24
Engineering & Computing
PC-PT
PC2
Printer-PT
Printer2
VLAN 30
192.168.3.0/24
2950T-24
Arts
PC-PT
PC3
ARTS
Printer-PT
Printer3
VLAN 40
192.168.4.0/24
2950T-24
Stud LAB
PC-PT
PC4
Printer-PT
Printer4
Stud LAB
VLAN 50
192.168.5.0/24
IT Dept
2950T-24
IT-Dept
PC-PT
PC5
Server-PT
FTP Server
Server-PT
Web Servier
VLAN 60
192.168.6.0/24


Cisco Packet Tracer - C:\Users\Sohan\Cisco Packet Tracer 8.2.2\saves\Virtual internship\jodCampus.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
CLOUD
20.0.0.0/30
10.10.10.4/30
10.10.10.0/30
Server-PT
Email-Server
2911
Cloud
2911
MAIN Chandigarh University Campus Router
SOUTH Campus
2911
Router2
AIT-CSE&Maths
Science
staff
2950T-24
Switch9
Printer-PT
Printer5
VLAN 70
192.168.7.0/24
PC-PT
PC6
3650-24PS
Multilayer Switch1
2950T-24
Switch10
PC-PT
PC7
VLAN 80
192.168.8.0/24
Printer-PT
Printer6
Stud-lab
Block B1
Block B2
Block B3
3650-24PS
Main Switch
Admin
2950T-24
Admin
PC-PT
PC0
Printer-PT
Printer0
VLAN 10
192.168.1.0/24
HR
2950T-24
HR
PC-PT
PC1
Printer-PT
Printer1
VLAN 20
192.168.2.0/24
E&C
2950T-24
Engineering & Computing
PC-PT
PC2
Printer-PT
Printer2
VLAN 30
192.168.3.0/24
2950T-24
Arts
PC-PT
PC3
ARTS
Printer-PT
Printer3
VLAN 40
192.168.4.0/24
2950T-24
Stud LAB
PC-PT
PC4
Printer-PT
Printer4
Stud LAB
VLAN 50
192.168.5.0/24
IT Dept
2950T-24
IT-Dept
PC-PT
PC5
Server-PT
FTP Server
Server-PT
Web Server
VLAN 60
192.168.6.0/24
Time: 02:45:30
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
Failed
PC1
PC0
ICMP
0.000
N
0
(edit)
(delete)
Failed
PC0
PC2
ICMP
0.000
N
1
(edit)
(delete)





Key Components:

Core Router: Central router connecting to the internet and managing traffic across different subnets.

Distribution Switches: Intermediate switches that aggregate traffic from multiple access switches.

Access Switches: Switches connecting end-user devices in classrooms, labs, and offices.

Firewalls: Positioned between the core router and the internet, and between core router and internal network segments to filter traffic.

Servers: Including web servers, file servers, database servers, etc.

End-User Devices: PCs, printers.

2. Security Assessment Report

Security Risks Identified:

- **Unauthorized Access**
- **Risk:** Weak or default passwords on network devices.
- **Countermeasure:** Implement strong password policies, regular password changes, and multi-factor authentication (MFA).

- **Data Breaches**
- **Risk:** Unencrypted sensitive data in transit.
- **Countermeasure**: Utilize encryption protocols such as SSL/TLS for data transmission and VPNs for remote access.

- **Network Availability**
- **Risk:** Single points of failure in network infrastructure.
- **Countermeasure:** Redundancy in network design, including backup routes and devices.

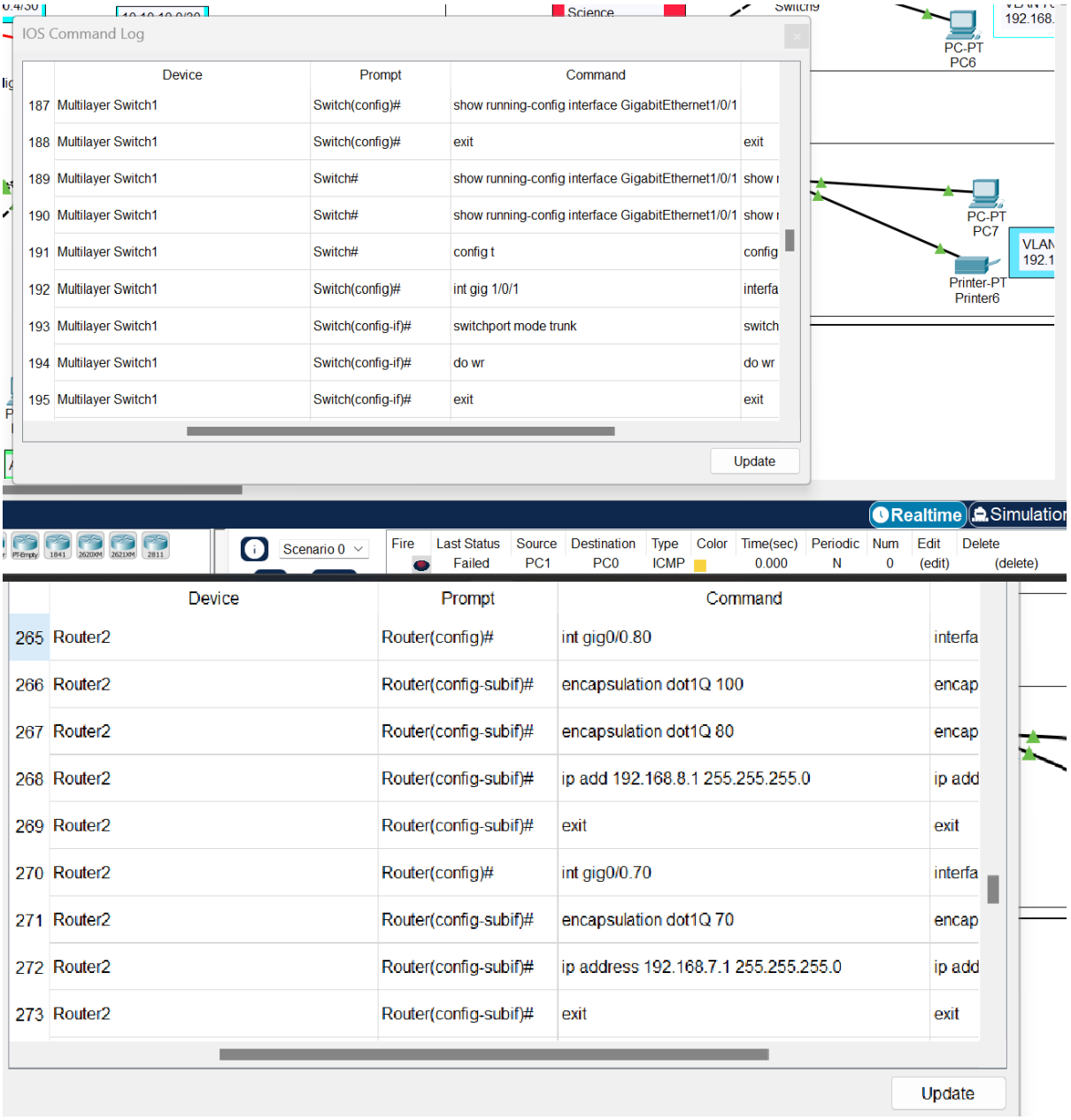
- **Malware and Ransomware**
- **Risk:** Malware infiltration through email or web browsing.
- **Countermeasure:** Deploy anti-malware solutions, regular software updates, and user education programs.

- **Physical Security**
- **Risk:** Unauthorized physical access to network devices.
- **Countermeasure:** Secure network rooms with access control systems, CCTV, and alarms.

Proposed Solutions and Countermeasures:

Implement Network Segmentation:

Create VLANs to segment traffic between different departments, reducing the attack surface and limiting the spread of potential threats.
(Check the github link to see the VLAN implementation)



Regular Network Audits and Penetration Testing:

Conduct regular security audits and penetration tests to identify vulnerabilities and ensure compliance with security policies.

Deploy Intrusion Detection and Prevention Systems (IDPS):

Install IDPS to monitor network traffic for suspicious activities and block malicious traffic in real-time.

Establish Incident Response Plan:

Develop and implement an incident response plan to quickly respond to and mitigate the impact of security breaches.
Continuous Monitoring and Logging:

Implement continuous monitoring solutions and maintain comprehensive logs of network

activities to detect and respond to anomalies.

By following these recommendations, the college campus network can improve its security posture, mitigate potential attack vectors, and enhance overall network resilience.

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:

Step 1: Explore Options for Hybrid Network Security

VPNs (Virtual Private Networks):

- Provide secure remote access for faculty and students.
- Ensure campus services are accessible only through the VPN.

Zero Trust Network Access (ZTNA):

- Enforce strict access controls regardless of network location.
- Provide secure access to applications based on user identity and context.

Endpoint Security Solutions:

- Deploy endpoint security software on faculty laptops to protect against threats.
- Use mobile device management (MDM) solutions to manage and secure student devices.

Step 2: Update Campus Network Topology

Add New Components:

- **VPN Gateways:** Integrate VPN gateways for remote access.
- **ZTNA Infrastructure:** Implement ZTNA components for secure access control.
- **Endpoint Security:** Ensure all faculty laptops and student devices have appropriate

security software.

-

Step 3: Explain Reasoning

VPN Advantages:

- Secure remote access to campus resources.
- Encryption ensures data security.

ZTNA Advantages:

- Enhanced security by verifying every access request.
- Reduces the risk of lateral movement within the network.

Endpoint Security:

- Protects devices from malware and other threats.
- Ensures compliance with security policies

Web Filtering Solutions:

- Use web filtering appliances or cloud-based solutions to control access to web content.
- Implement solutions like Cisco Umbrella or Fortinet FortiGuard Web Filtering.

Proxy Servers:

- Deploy proxy servers to monitor and filter web traffic.
- Configure access control lists (ACLs) to block irrelevant sites.

DNS Filtering:

Use DNS filtering to block access to specific categories of websites.

Step 2: Update Campus Network Topology

Add New Components:

Web Filtering Appliance: Integrate a web filtering solution into the network.

Proxy Servers: Add proxy servers for traffic monitoring and filtering.

DNS Filtering: Implement DNS filtering for content control.

Step 3: Explain Reasoning

Web Filtering Advantages:

- Granular control over web content access.
- Protects against malicious websites.

Proxy Server Advantages:

- Monitors and controls web traffic.
- Provides detailed reports on web usage.

DNS Filtering:

- Simple to implement.

- Effective at blocking categories of websites.

Policies:

Web Filtering Policy: Block access to social media, streaming services, and other non-educational content during class hours.

Proxy Server Policy: Monitor and log all web traffic, block access to unauthorized sites.

DNS Filtering Policy: Implement category-based filtering to block inappropriate content.

Conclusion

By following these steps and implementing the proposed solutions, the college can enhance its network security, support a hybrid working environment, and restrict access to irrelevant web content, ensuring a secure and focused learning environment.

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)

Network Security Solutions for Campus Networks

1. Web Content Filtering Solutions

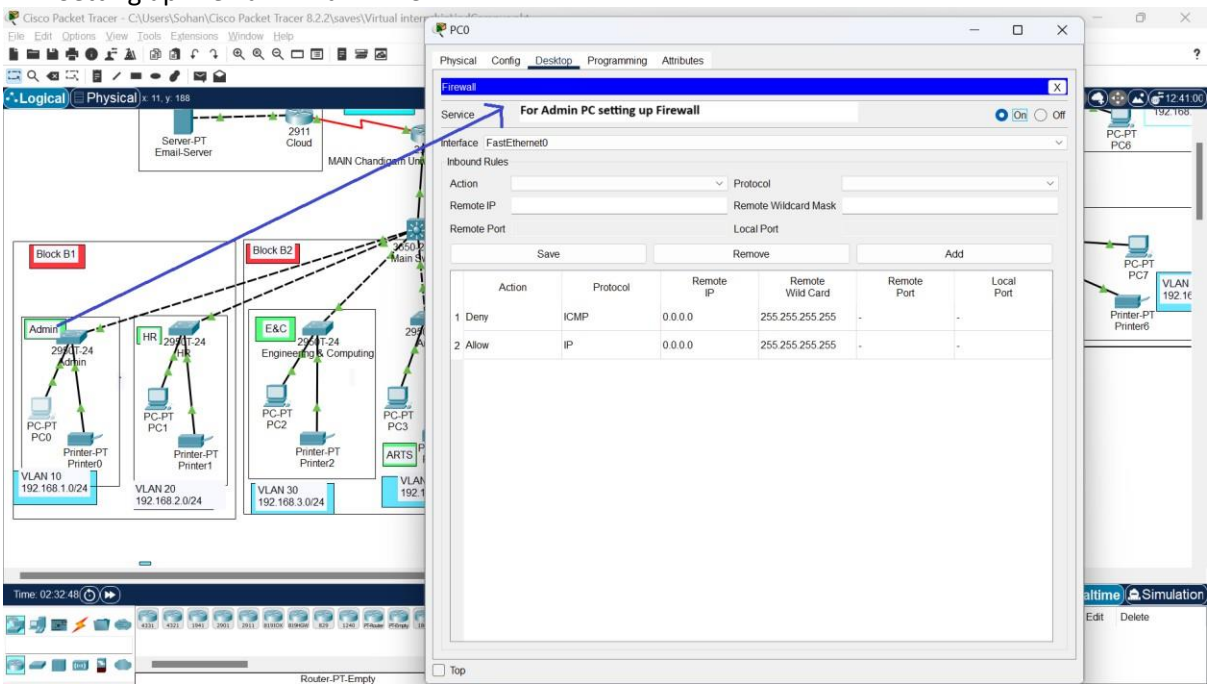
- **Product Example: Cisco Umbrella**
- **Use**: Provides DNS-based security by blocking access to websites based on categories, security risks, or specific URLs, ensuring that only approved content is accessible.

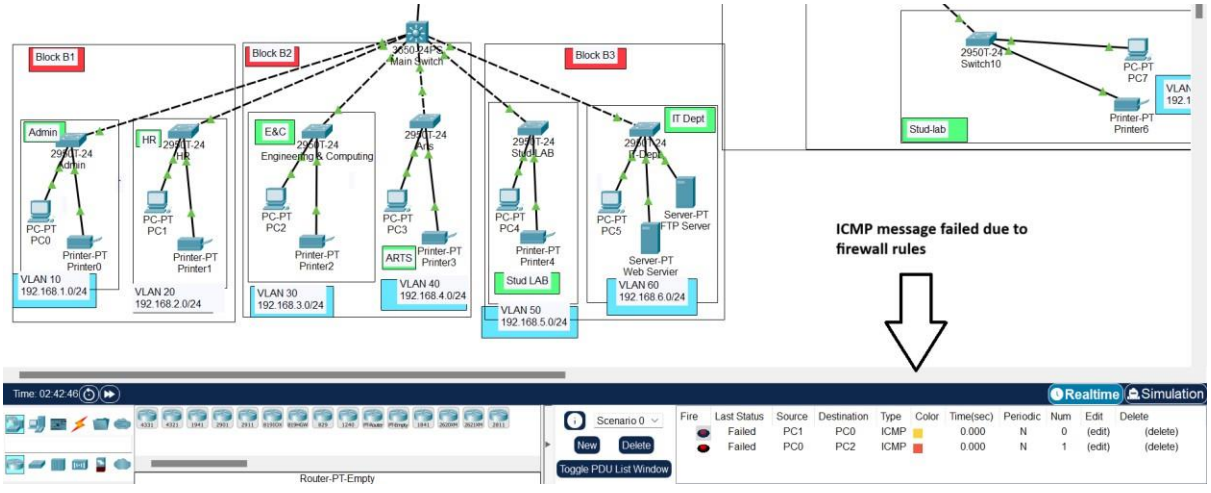
2. Firewall with Integrated Security Services

- **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

- Setting up firewall in Admin PC





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

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:

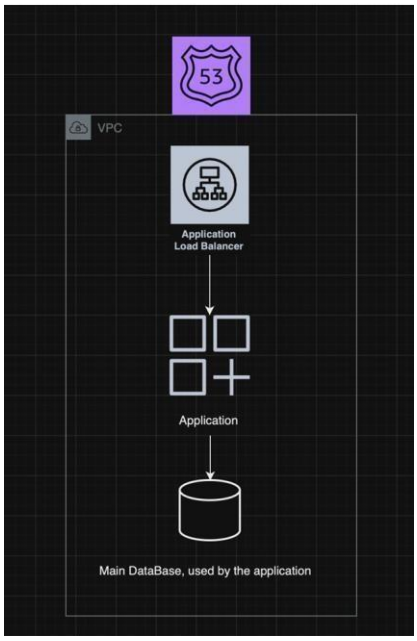
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

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. Enhancing System Availability:

- **Load Balancing:** Utilize an elastic load balancer to distribute incoming web traffic across multiple servers, ensuring high availability and fault tolerance by preventing any single server from becoming overloaded.

- **Auto-Scaling:** Automatically scale the number of instances based on demand, such as during flash sales, to avoid performance bottlenecks.

2. Ensuring Database Scalability and Reliability:

- **Database Clustering:** Implement a clustered environment with primary and replica databases to ensure high availability. The replica can handle read requests and serve as a failover solution.

- Enable real-time data replication to a secondary database and perform regular snapshots for quick restoration in case of data corruption.

3. **Efficiently Handling Burst Traffic:**

- **Content Delivery Network (CDN):** Deploy a CDN to cache static content at edge locations, reducing load times and server load during high traffic periods.

- **Caching Strategies:** Use Redis or Memcached to serve frequently accessed data, minimizing repeated database queries.

4. **Mitigating DDoS Attacks:**

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

Updated Cloud Architecture Diagram:

- Load Balancer: Distributes traffic across web servers.
- Auto-Scaling Group: Dynamically adjusts resources based on demand.
- WAF and DDoS Protection: Serve as the first line of defense against attacks.
- Database Cluster: Ensures availability with primary and replica databases.
- CDN and Caching Layers: Reduce latency and server load during peak traffic.

By implementing these strategies, your startup can achieve resilience, scalability, and security for its e-commerce platform, effectively addressing current challenges and preparing for future growth.