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.

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 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

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)

Cloud Security

Problem Statement:

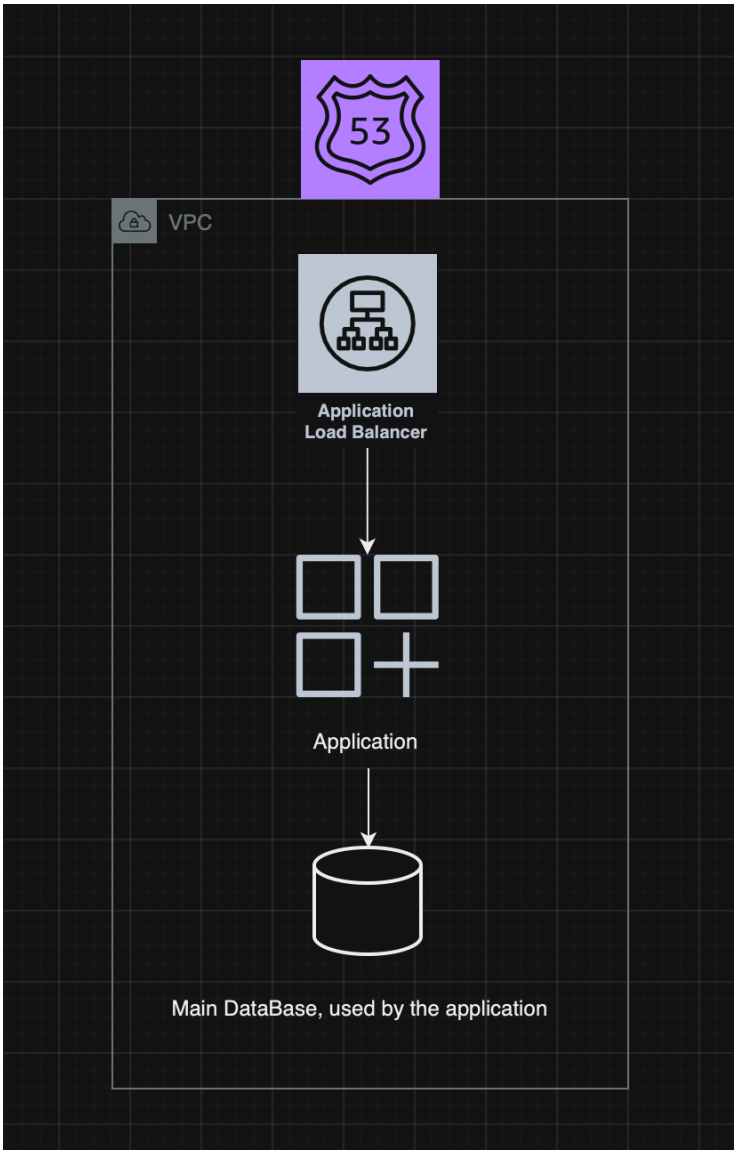
You have been hired as a cloud architect by a start-up. The start-up is an ecommerce retailer which has popular sale days on regional festivals or holidays.

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.