College Name	**University of Hertfordshire SEGi College Subang Jaya**		
Programme Name	**BACHELOR OF SCIENCE (HONS) COMPUTER SCIENCE (CYBER SECURITY AND NETWORKS)**		
Module Name	**CYBER SECURITY AND NETWORKS PROJECT**	Module Code	**6COM1040**
		Semester	**September 2025**
Module Leader	**Dr. Aneshkumar Thangaveloo**	Assessment Type	**System Architecture Diagram**
Lecturer Name	**Ms. Nur Diana Madinah Binti Ab Hadi**		
Student's declaration	I hereby certify that this assignment is my own work and where materials have been used from other resources, they have been properly acknowledged. I also understand I will face the possibility of failing the module if the content of this assignment is plagiarized.		

No.	**Name**	**Student ID**	**Signature / Initial**
1	PATRICK ROGERS	SCSJ2100424	PAT

Date:

Release Date		Submission Due Date		Marks obtained:
Date Received		Student's work assessed by / date		

Module Leader’s Feedback.

Module Leader’s comments / feedback	
Student’s comments	

Table of Contents

Table of Figures

1.0 System Design and Security Analysis

A2Z Corporation operates an internet-facing environment that hosts essential services required by external clients, internal employees, and administrative staff. Due to its online exposure and interconnected systems, the organization faces multiple cybersecurity risks that must be mitigated through proper architectural design and layered defence methods. The most significant risks include external cyberattacks (such as port scanning, reconnaissance, brute-force attempts, and exploitation of public-facing services), man-in-the-middle attacks, service disruptions, unauthorized access into the internal network, and zero-day vulnerabilities affecting running services such as web servers or containerized applications.

To address these threats, the designed system architecture adopts a segmented, defence-in-depth security model using a DMZ (Demilitarised Zone), host-level firewall, intrusion detection system (IDS), and container isolation. The DMZ hosts the Ubuntu server running the OWASP Juice Shop web application, while the internal LAN contains only administrative systems. A router acts as the boundary between the internal network, DMZ, and the simulated cloud environment. This structure significantly reduces the attack surface by preventing direct access to internal computers while still enabling secure access to needed services.

The architecture diagram (Figure 1) illustrates how the components are organised and secured within the network.

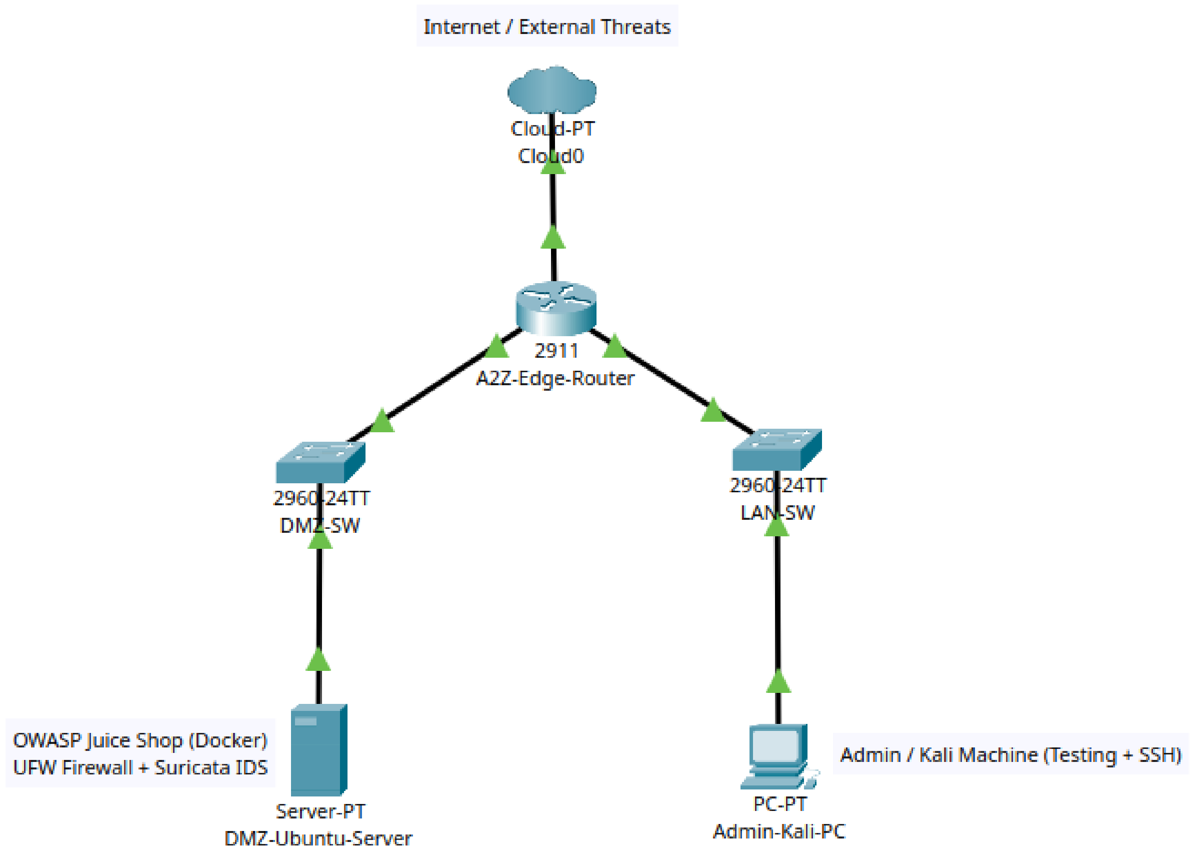
Internet / External Threats
Cloud-PT
Cloud0
2911
A2Z-Edge-Router
2960-24TT
DMZ-SW
2960-24TT
LAN-SW
OWASP Juice Shop (Docker)
UFW Firewall + Suricata IDS
Server-PT
DMZ-Ubuntu-Server
Admin / Kali Machine (Testing + SSH)
PC-PT
Admin-Kali-PC

Figure 1: System Architecture Diagram

The diagram shows the following main components:

- **Cloud/Internet** - external environment where potential attackers originate.
- **A2Z-Edge-Router** - isolates and manages traffic flow between DMZ, internal LAN, and cloud.
- **DMZ-SW** - connects the Ubuntu server that hosts the web application.
- **LAN-SW** - connects the admin PC, which performs system management and testing.
- **DMZ-Ubuntu-Server** - hosts Juice Shop using Docker; protected by UFW firewall and monitored by Suricata IDS.
- **Admin-Kali-PC** - used for controlled security testing and administrative access.

1.1 IP Address Plan (Simulation Only)

Network Segment	Subnet	Router Gateway	Device	IP Address
DMZ	192.168.10.0/24	192.168.10.1	Ubuntu Server	192.168.10.10
Internal LAN	192.168.20.0/24	192.168.20.1	Admin PC (Kali)	192.168.20.10
WAN / Internet	10.0.0.0/24	10.0.0.1	N/A	N/A

1.2 Plan Firewall Policies

Source	Destination	Port / Protocol	Action
Internet	DMZ Server	80, 443 (HTTP/HTTPS)	ALLOW
Internet	Internal LAN	ANY	DENY
DMZ Server	Internet	80, 443	ALLOW (for updates only)
Internal LAN	DMZ Server	22 (SSH), 443	ALLOW
Internal LAN	Internet	ANY	ALLOW
DMZ Server	Internal LAN	ANY	DENY (prevent lateral movement)

This design directly addresses A2Z's most critical security concerns. First, external exposure risk is mitigated by ensuring that only the necessary ports are open on the DMZ server, with all other connections blocked by the firewall. Second, network intrusion and lateral movement risks are minimised by isolating the DMZ from the internal LAN. Even if the public-facing server is compromised, the attacker will not automatically reach internal systems. Third, monitoring and detection risks are handled through Suricata IDS running on the DMZ interface to detect suspicious traffic such as port scans, OS fingerprinting, and brute-force attempts.

Furthermore, containerisation through Docker enhances security by isolating the vulnerable web application from the underlying host operating system. Even if the container is compromised, the attacker does not gain root access to the host machine or the internal network.

Encryption measures such as HTTPS can be integrated to protect data-in-transit and mitigate the risk of interception. The UFW firewall ensures that no unnecessary inbound or outbound communication occurs, providing strict control over external access.

Finally, the system design follows established security principles such as least privilege, segmentation, isolation, and continuous monitoring. These choices align with A2Z Corporation’s security needs because they ensure that public services remain available while preventing unrestricted external access, detecting malicious behaviour early, and limiting damage in the event of an attack.