<table>
<tr><td>College Name</td><td colspan="3">University of Hertfordshire
SEGi College Subang Jaya</td></tr>
<tr><td>Programme Name</td><td colspan="3">BACHELOR OF CYBERSECURITY AND NETWORKS</td></tr>
<tr><td rowspan="2">Module Name</td><td rowspan="2">CYBERSECURITY</td><td>Module Code</td><td>6COM1040</td></tr>
<tr><td>Semester</td><td>SEP 2025</td></tr>
<tr><td>Module Leader</td><td>DR ANESHKUMAR THANGAVELOO</td><td rowspan="2">Assessment Type</td><td rowspan="2">PROJECT SYSTEM ARCHITECTURE DIAGRAM</td></tr>
<tr><td>Lecturer Name</td><td>MS NUR DIANA MADINAH</td></tr>
<tr><td>Student’s declaration</td><td colspan="3">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.
<table>
<tr><th>No.</th><th>Name</th><th>Student ID</th><th>Signature / Initial</th></tr>
<tr><td>1</td><td>TAN JIAJIAN</td><td>SCSJ1901781</td><td>TAN</td></tr>
</table></td></tr>
<tr><td>Release Date</td><td></td><td>Submission Due Date</td><td>8/12/2025</td><td rowspan="2">Marks obtained:</td></tr>
<tr><td>Date Received</td><td></td><td>Student’s work assessed by / date</td><td></td></tr>
</table>

Module Leader's Feedback.

Contents

List of Ligure

2. System Design and Security Analysis

Internet-Facing Security Risks

A2Z Corporation faces several security threats due to its public-facing services

1. Unauthorized Access to Internal LAN: Attackers may attempt to exploit misconfigured routers or open ports to access sensitive administrative systems.
2. Attacks on Public Web Server: The DMZ-hosted web server is exposed to potential threats such as DDoS attacks, force login attempts and web application vulnerabilities.
3. Malware and Phishing Attacks: External sources could attempt to introduce malware or phishing content into the network, threatening sensitive data.
4. Reconnaissance Activities: Cyber attackers may scan open ports or exploitable services, aiming to gather information for subsequent attacks.

System Architecture Diagram

The proposed network architecture uses segmentation, controlled access and traffic filtering to mitigate these risks.

1. Network Segmentation:
    - DMZ (192.168.10.0/24): Contains the web server (192.168.10.1/24). allow only HTTP (port 80) and HTTPS (port 443) to the internet.
    - Internal LAN (192.168.20.0/24): Contains Admin-PC (192.168.20.1/24). Fully isolated from inbound internet traffic.
    - The router interfaces are isolated networks: Gig0/0 connects to the internet (203.0.113.2), Gig0/1 to DMZ, and Gig0/2 to the internal LAN.
2. Firewall Policies:
    - Inbound to DMZ: Only HTTP (80) and HTTPS (443) traffic is allowed. All other ports are blocked.
    - Inbound to Internal LAN: Completely blocked.
    - Outbound to Internal LAN: The administrator PC can access the internet and DMZ to manage the web server.
3. Device Placement and Connectivity:
    - Internet (Cloud): IP 203.0.113.1 connected to router Gig0/0 via a copper straight-through cable.
    - Router: Edge router handling routing and firewall policies. Interfaces:

    - G0/0 → Cloud
    - G0/1 → SW-DMZ
    - G0/2 → SW-LAN
- Switches:
    - SW-DMZ connects to router G0/1 and DMZ-WebServer FastEthernet0.
    - SW-LAN connects to router G0/2 and Admin-PC FastEthernet0.
- Server: Ubuntu web server in DMZ, IP 192.168.10.1.
- Admin-PC: Internal workstation, IP 192.168.20.1.
- Cables: All copper straight-through.
- Security:
    - Firewall configured on router interfaces (G0/0, G0/1, G0/2).
    - Only required ports open, DMZ exposed to HTTP/HTTPS, internal LAN isolated.

4. Encryption and Monitoring:
    - HTTPS (port 443): Ensures encrypted traffic between external users and the web server.
    - Potential IDS/IPS in Packet Tracer simulation: Can monitor unusual traffic in DMZ and internal LAN, alerting administrators to intrusion attempts.

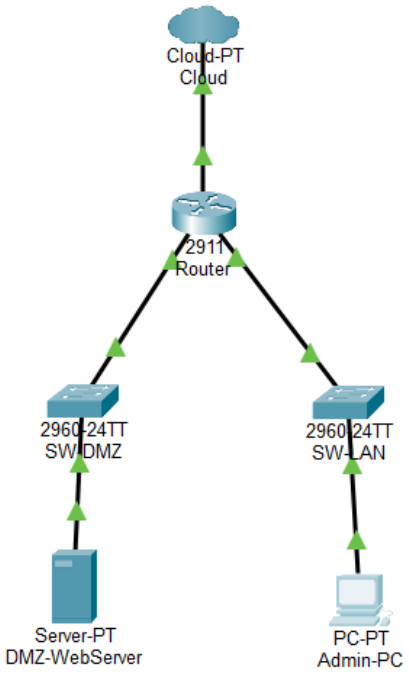

Figure 1

Justification of design choices

1. Segmentation: Separating DMZ from the internal LAN ensures that even if the web server is compromised, the core administrative systems remain protected.
2. Controlled Access: By allowing only essential ports and blocking all other traffic, the network reduces the attack surface and prevents common exploits.
3. Routing and Firewall Placement: Placing the firewall rules on router simplifies traffic control and ensures a central point of policy enforcement.
4. Encrypted Traffic: Using HTTPS ensures data confidentiality for clients accessing public services, mitigating risks of eavesdropping or data tampering.

Future IDS/IPS Integration: Although optional in Packet Tracer, adding monitoring systems would enhance detection of abnormal activities and support proactive security.