A2Z CORPORATION: SECURE NETWORK DEFENSE ARCHITECTURE

NAME: PATRICK ROGERS

STUDENT ID: SCSJ2100424

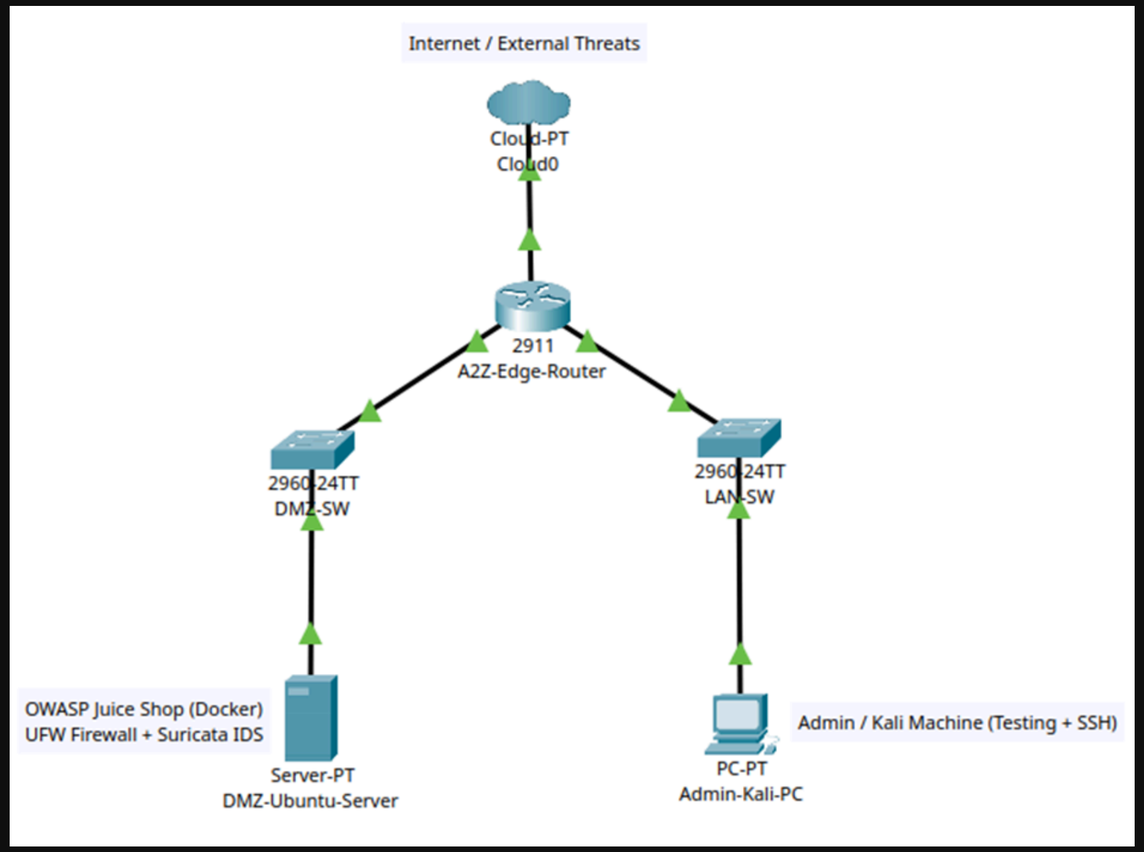
SYSTEM DESIGN

KEY ARCHITECTURAL FEATURES

Purpose: Mitigate risks like external attacks and lateral movement by isolating network segments.

- **Demilitarized Zone (DMZ):** Hosts the public-facing service (Ubuntu Server/Juice Shop).
- **Internal LAN:** Protected segment for administrative systems (Admin-Kali-PC).
- **Boundary Control:** A2Z-Edge-Router manages traffic flow and enforces strict isolation policies.

This structure prevents direct access to internal assets from the internet.



NETWORK SEGMENTATION & IP PLAN

IP ADDRESSING AND COMPONENTS

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

Internet - DMZ: ALLOW ports 80, 443 (Least Privilege).

Internet - Internal LAN: DENY ALL (Isolation).

DMZ - Internal LAN: DENY ALL (Prevent Lateral Movement).

Internal LAN - DMZ: ALLOW SSH/443 (Administrative Access).

IMPLEMENTED SECURITY MEASURES: UFW FIREWALL

HOST-LEVEL ACCESS CONTROL

Default Policy: Deny ALL incoming traffic.

Allowed Ports: Explicitly enabled only 80, 443, 3000.

SSH Restriction: Port 22 is restricted solely to the trusted Admin-Kali-PC IP (192.168.20.10).

Function: Acts as the first line of defense, strictly controlling network traffic and minimizing the server's attack surface against brute-force and exploitation attempts.

IMPLEMENTED SECURITY MEASURES: DOCKER

APPLICATION ISOLATION AND CONTAINMENT

Application: OWASP Juice Shop deployed in a Docker container (exposed on port 3000).

Security Benefit: Isolation. Contains potential breaches within the container, preventing attackers from gaining root access to the host OS or moving laterally.

Resilience: Malicious changes are non-persistent and automatically erased when the container is restarted.

IMPLEMENTED SECURITY MEASURES: SURICATA IDS

REAL-TIME THREAT DETECTION

Deployment: Installed and configured to monitor the DMZ interface (enp0s8).

Detection Capability:

- Identifies port scans (like Nmap).
- OS fingerprinting.
- Brute-force attempts.

Role: Provides continuous monitoring and early warning, detecting threats that bypass the host-level firewall.

SECURITY TESTING & VALIDATION

NMAP SCANNING

Method: Simulated an external attacker to confirm firewall rules and network mapping.

Result: Only expected ports (80, 3000) were open. Services were successfully enumerated, confirming visibility controls.

SURICATA IDS ALERTS

Method: Monitored IDS logs during the Nmap simulation.

Result: 78 alerts generated. The IDS is fully functional in real-time detection mode.

CONCLUSION

PROJECT SUMMARY: ENHANCED SECURITY POSTURE

A secure, layered infrastructure was successfully designed, implemented, and validated for A2Z Corporation. Key outcomes include:

- Reduced Attack Surface (UFW + DMZ segmentation).
- Isolated Vulnerable Services (Docker containerization).
- Continuous Threat Detection (Suricata IDS).

The system is now more resilient and secure against key external threats, providing enhanced operational continuity.

THANK YOU