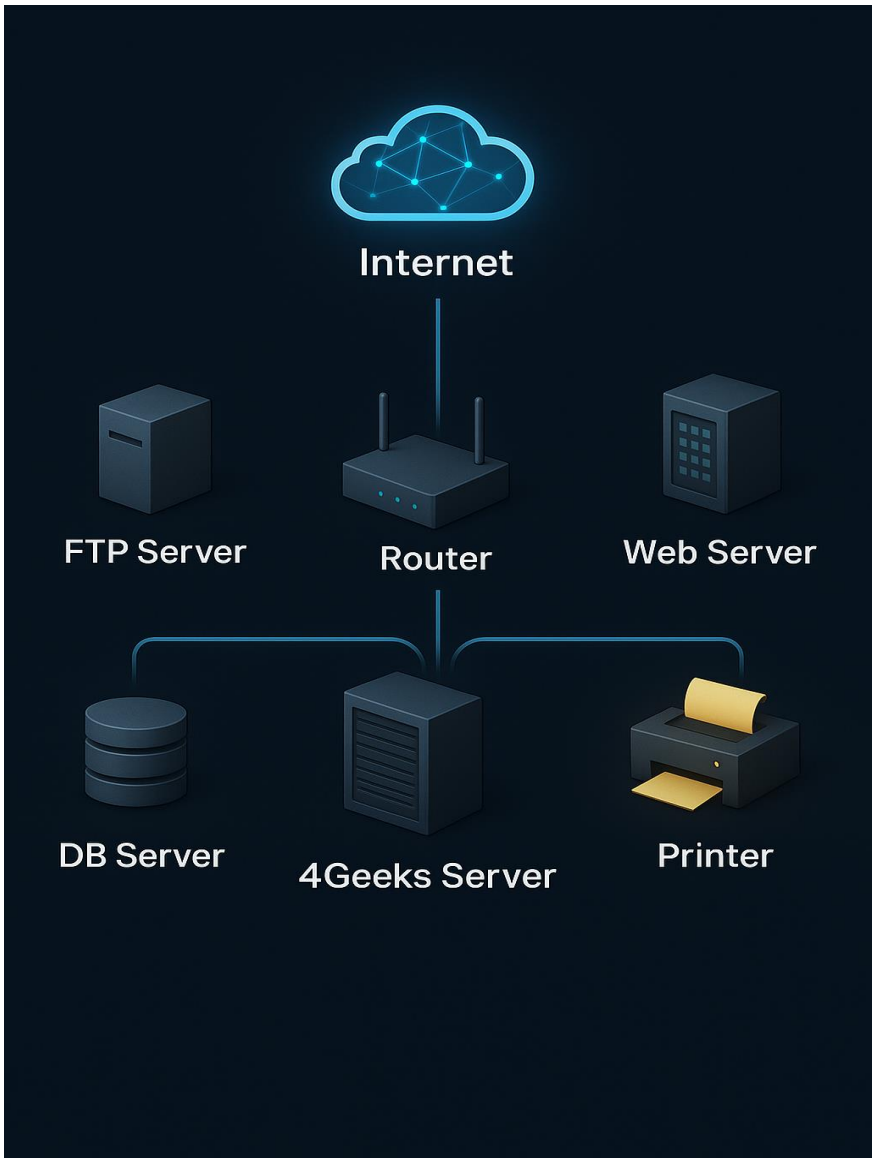
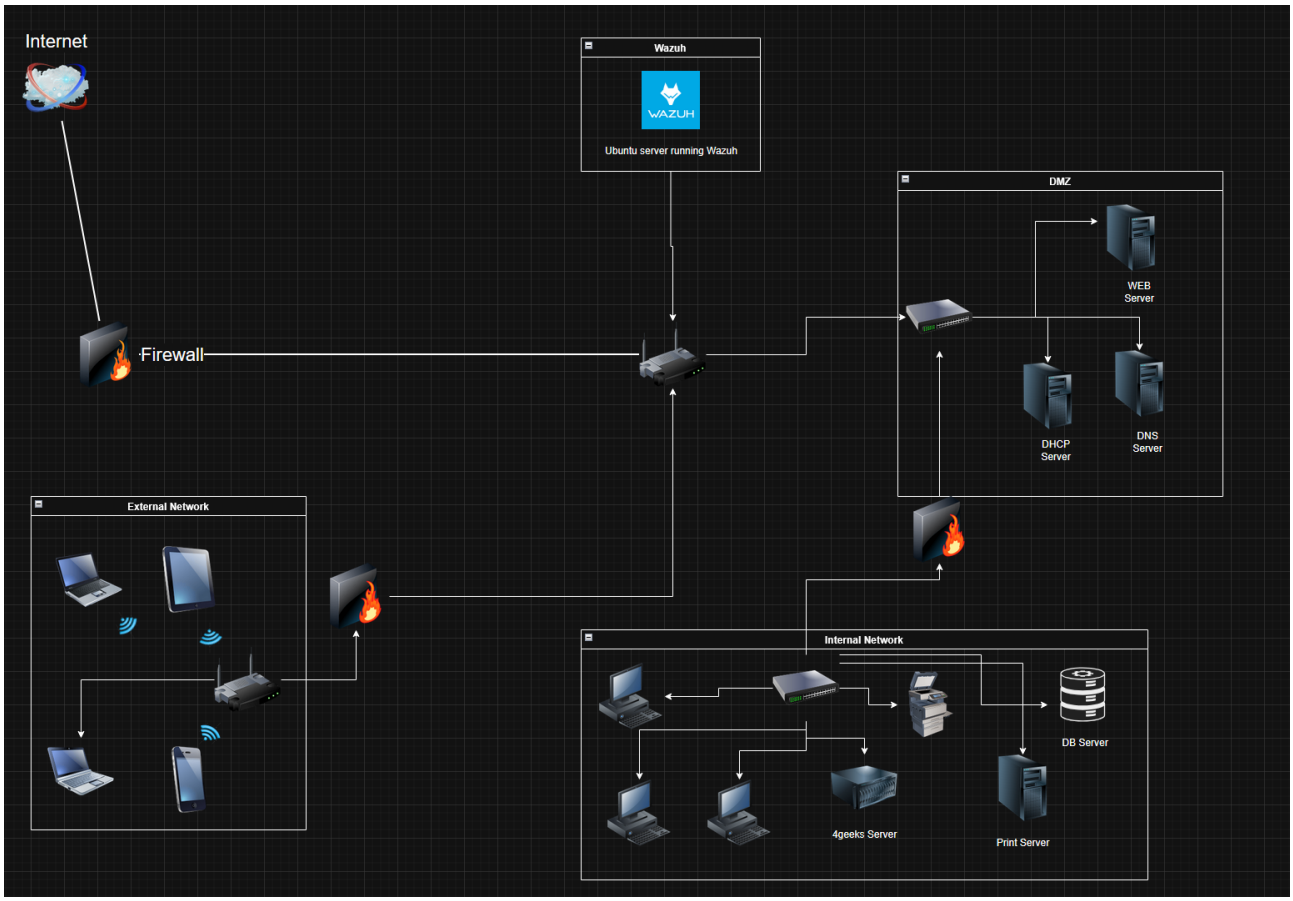
Network Diagram

Actual



From my assessment, there appears to be no active firewall in place, leaving the environment significantly exposed. Unauthorized access points are easily identifiable through basic network enumeration techniques such as **Nmap scanning**, indicating a lack of fundamental perimeter defense and traffic filtering. This represents a critical security gap that must be addressed to prevent external threats and lateral movement within the network.

The ideal network architecture should be designed based on best practices for security and operational efficiency; however, it must also align with the **budgetary constraints and business requirements** of each organization. A cost-effective solution can still provide strong segmentation, access control, and monitoring capabilities when planned and prioritized appropriately.



To enhance network security, I have implemented additional firewalls and segmented the infrastructure into distinct zones. This allows for the application of granular access controls and the enforcement of the **principle of least privilege**. By applying **role-based access control (RBAC)**, users are assigned appropriate permissions based on their roles, ensuring proper governance and minimizing unnecessary access.

Furthermore, the integration of an **Extended Detection and Response (XDR)** solution provides centralized visibility across the environment. It enables real-time threat detection, automated alerting, and response capabilities through predefined rules, ensuring prompt mitigation of potential attacks.