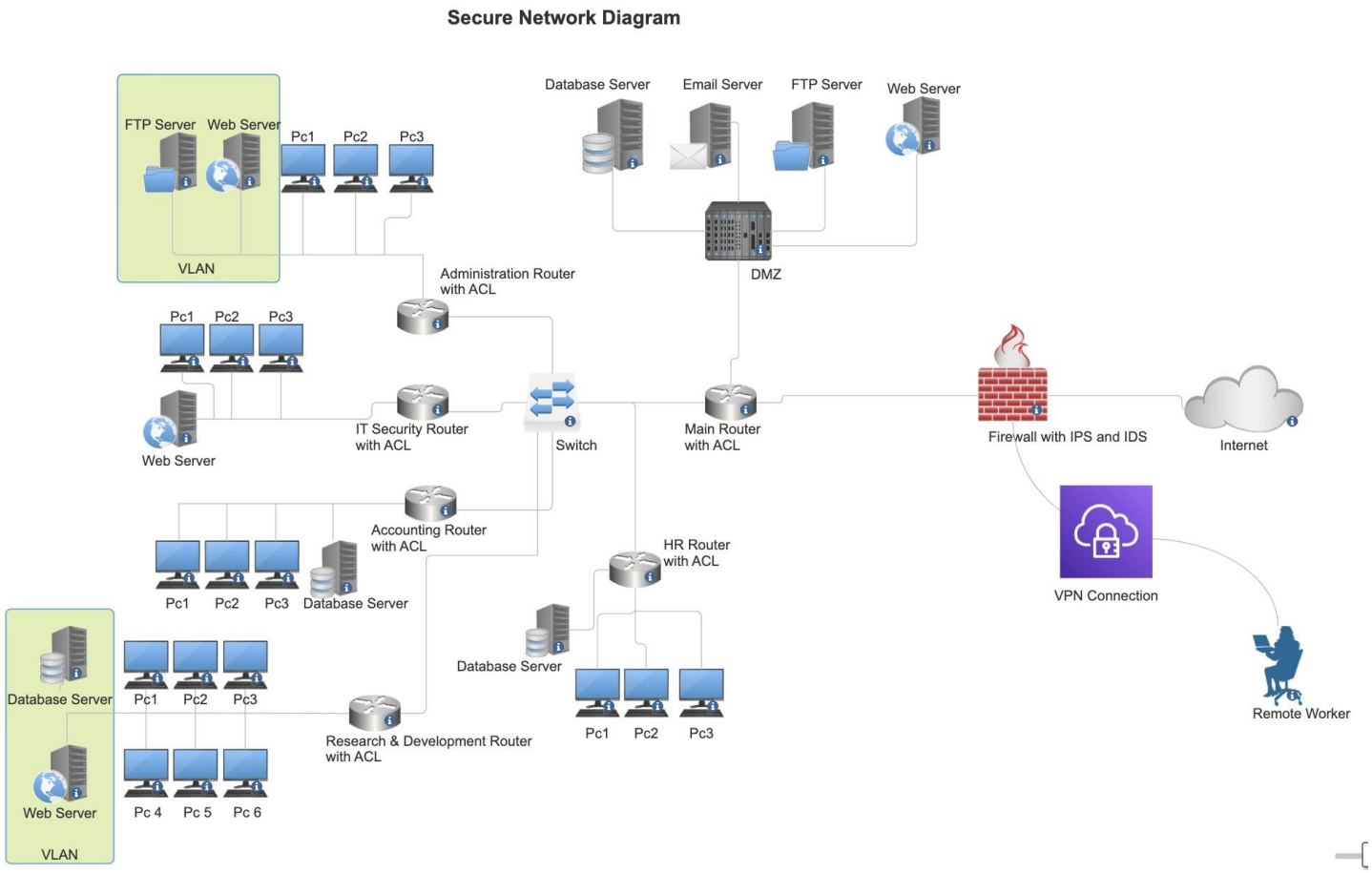
Secure Network Diagram



Security Features Implemented:

- DMZ
- VLAN
- VPN
- Access Control Lists (ACL)
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- FireWall
- Multi Factor Authentication(MFA)

The provided network diagram represents a Mid Size IT Company with various departments, including Accounting, HR, Research and Development, IT security, and Administration. Each department is treated as a subsystem within the network. Additionally, a **Demilitarized Zone (DMZ)** is integrated, housing servers like the Mail Server, Database Server, and FTP server. These servers are accessible to both internal and external users but are designed to mitigate damage in case of a compromise, limiting access to the internal network.

Within the DMZ, there's a Database Server, and each department also has dedicated database servers. These department-specific servers only accept requests from computers within their respective subsystems, ensuring that restricted data remains inaccessible to unauthorized personnel. This approach simplifies authorization management and minimizes the risk of data breaches, as employees only have access to relevant resources.

The servers within each department is further secured using a **VLAN** to prevent attackers from gaining access

through phishing attack on employees computer. **Access control Lists** on the routers restrict unauthorized users from accessing business-sensitive information. It also controls network traffic by limiting the number of users accessing files, systems, and information. This increases network performance and helps protect business information.

To enable remote work, employees must connect through a secure **virtual private network** (VPN), requiring a username, password, and a periodically changing RSA token installed on company-provided laptops. The Administration department receives the highest level of security due to the sensitivity of its data. A dedicated FTP server is provided to facilitate file sharing within the department while restricting access for employees from other departments and external sources.

The network architecture involves connecting each department's router to a main router via network switches. The main router is linked to a firewall. The Firewall is equipped with **intrusion prevention system (IPS)** and **Intrusion Detection System (IDS)**. IPS and IDS monitors all traffic on the network to identify any known malicious behavior and blocks them before they successfully compromise any endpoints within the network