Secure Network Architecture Overview

Key Security Components

- **Frontend Firewall (NGFW) :**
  The Next-Generation Firewall (NGFW) acts as the first line of defence between the internet and the organization's internal network. It controls access to the DMZ and performs deep packet inspection, VPN management, malware protection, and application-level filtering. This helps financial institutions meet regulatory and security standards.
- **DMZ (Demilitarized Zone)**
  The DMZ isolates public-facing services (e.g., web servers, email servers) from the internal network. This reduces the attack surface and prevents direct access to sensitive financial data in the event of a compromise.
- **Backend Firewall**
  An internal firewall adds an extra layer of protection between the DMZ and core internal systems, limiting lateral movement in case of intrusion and enforcing network segmentation.
- **Web Application Firewall (WAF)**
  A WAF filters HTTP traffic to prevent common web-based attacks such as SQL Injection, Cross-Site Scripting (XSS), and Distributed Denial-of-Service (DDoS). This is crucial for protecting web applications in the DMZ.
- **NIDS & NIPS:** Deployed behind the backend firewall, Network Intrusion Detection and Prevention Systems monitor and react to suspicious traffic:
  - NIDS alerts administrators to anomalies
  - NIPS automatically blocks threats in real time
- **Network Segmentation**
  - VLANs
    Virtual LANs (VLANs) segment internal departments (e.g., Finance, R&D, Management), limiting the spread of malware and restricting unauthorized access. Segmentation enhances visibility and simplifies compliance audits.
- **Access and Data Protection**
  Multi-Factor Authentication (MFA) MFA adds an additional verification layer to protect against phishing and credential compromise.
- **Encryption**
  Encryption secures data in transit and mitigates Man-in-the-Middle (MITM) attacks by ensuring only authorized parties can read communication - aligning with the Confidentiality, Integrity, and Availability (CIA) triad.

Project Context

This design was originally developed as part of my MSc in Cybersecurity. It has since been restructured and documented to showcase practical knowledge in enterprise network security and architectural planning.