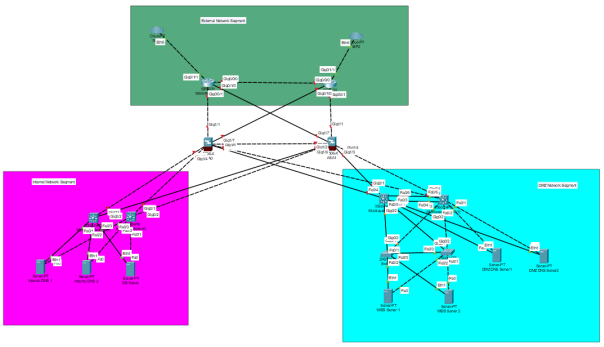
Design a Secure Network Architecture



NGFW (Next Generation Firewall)

> Provides advanced threat protection, deep packet inspection, and application awareness to secure the network perimeter.

Router

> Routes data packets between networks, directing traffic within the internal network and to external networks.

Switches

> Connects devices within a local area network (LAN) and efficiently forwards
> data to the correct device.

HIDS (Host Intrusion Detection System)

> Monitors individual hosts for suspicious activity and potential security breaches, alerting administrators.

NIDS (Network Intrusion Detection System)

> Monitors network traffic for signs of malicious activity or policy violations, providing early detection of attacks.

DHCP (Dynamic Host Configuration Protocol)

> Automatically assigns IP addresses to devices on the network, simplifying network management.

File Servers

> Provide centralized storage and access to files and documents for users and applications.

Database Servers

> Manage and store structured data, handling requests from applications and users for data retrieval and manipulation.

Policy Servers

> Enforce security policies and access controls across the network, ensuring compliance with organizational standards.

Web Servers

> Host websites and web applications, serving content to users over the internet or an intranet.

Directory Services

> Manage user identities and access permissions, allowing for centralized authentication and authorization.

Internally Used Apps

> Applications that are essential for business operations, typically hosted on internal servers and accessed by employees.

NIPS(Network Intrusion Prevention System)

> Actively blocks malicious traffic by analyzing packets in real-time, preventing threats before they enter the network. Positioned inline, it stops or drops packets that match attack signatures.