Mariam Mostafa Amin

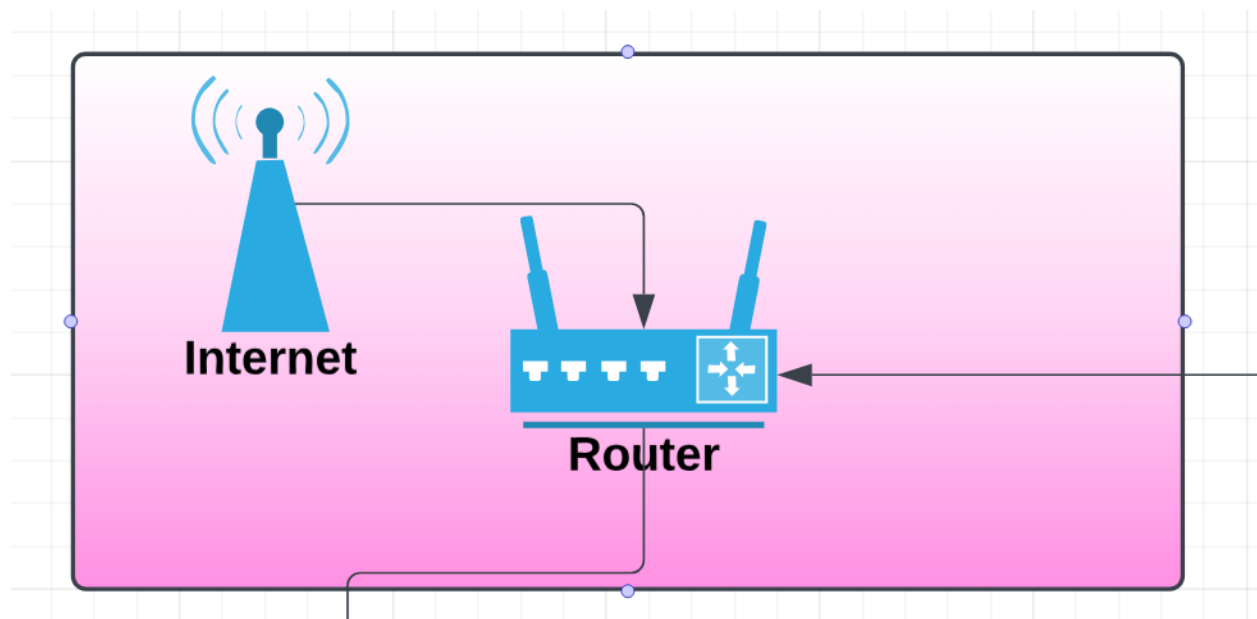--
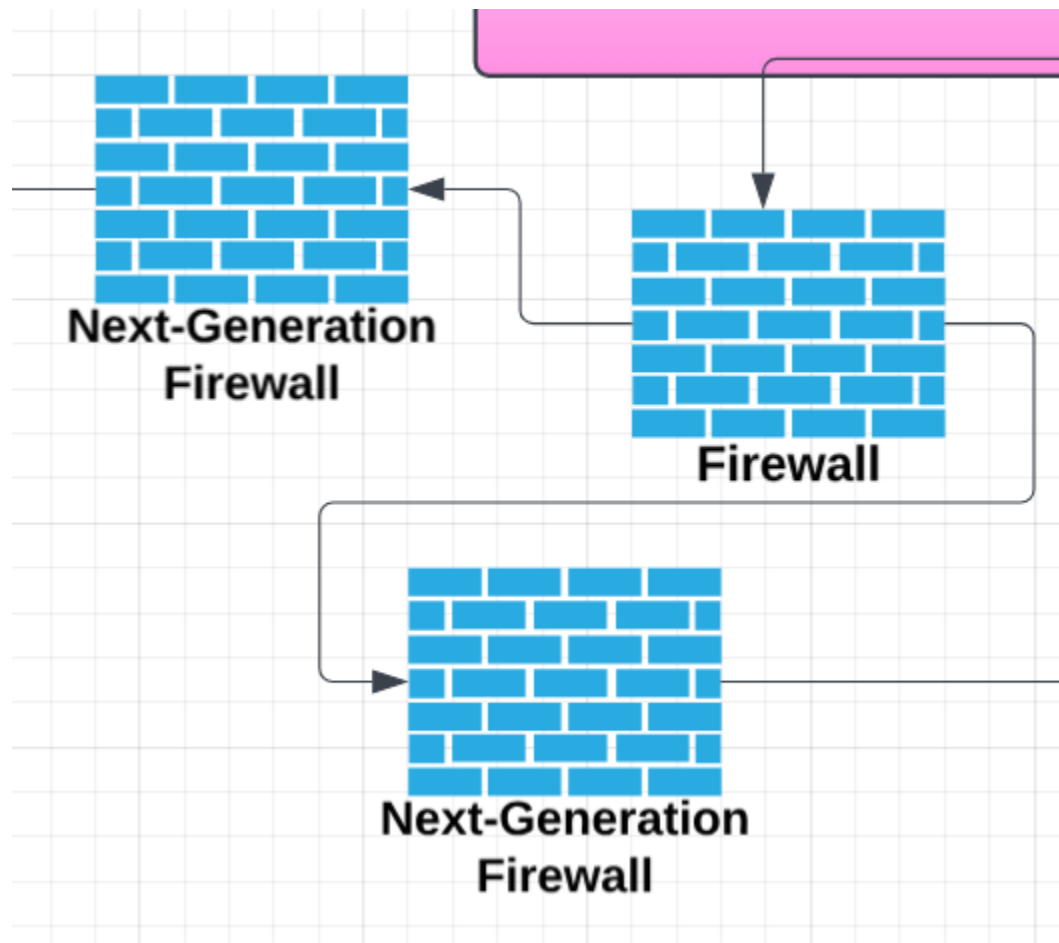
Internet Zone:

Internet: The Public Worldwide Internet to be connected to access data

Router: My Internet Router which will be connected to my Secure System and connected to my internal network
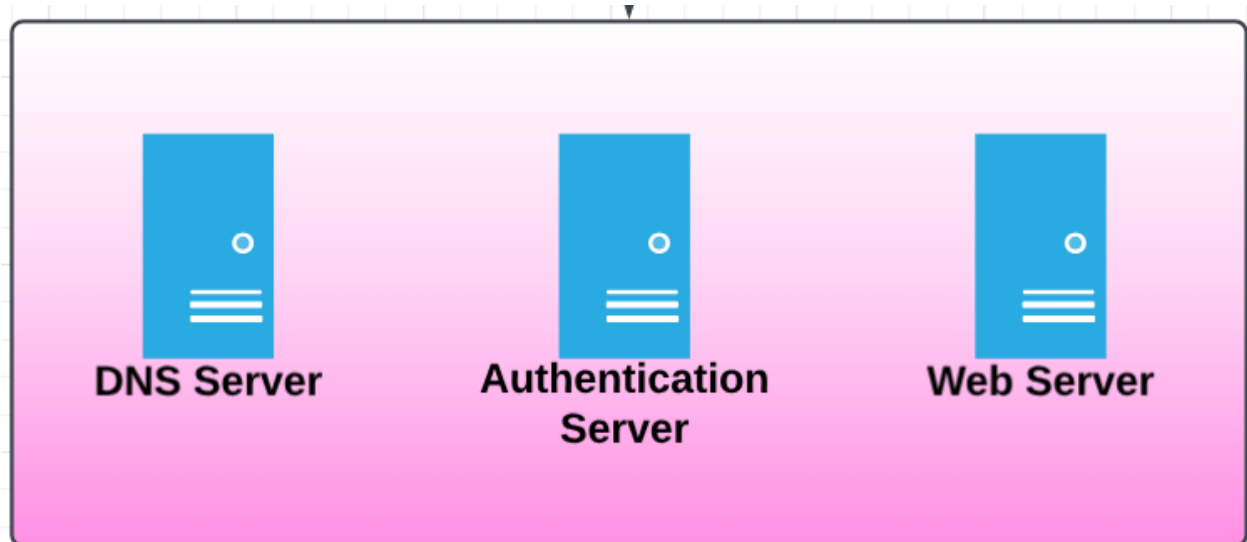
Firewalls:

Firewall: Control and filters the outcoming and incoming network traffic based on the security rules

Next-Generation Firewall: An advanced firewall that provides deep packet inspection and can detect threats at the application layer

DMZ:

DNS Server: A system that translates domain names like (www.facebook.com) into IP addresses, allowing devices to locate resources on the network or the internet

Authentication Server: Systems like Active Directory or RADIUS that verify user identities, ensuring that only authorized users can access network resources

Web Server: hosting and serving web applications or websites

Internal Network:
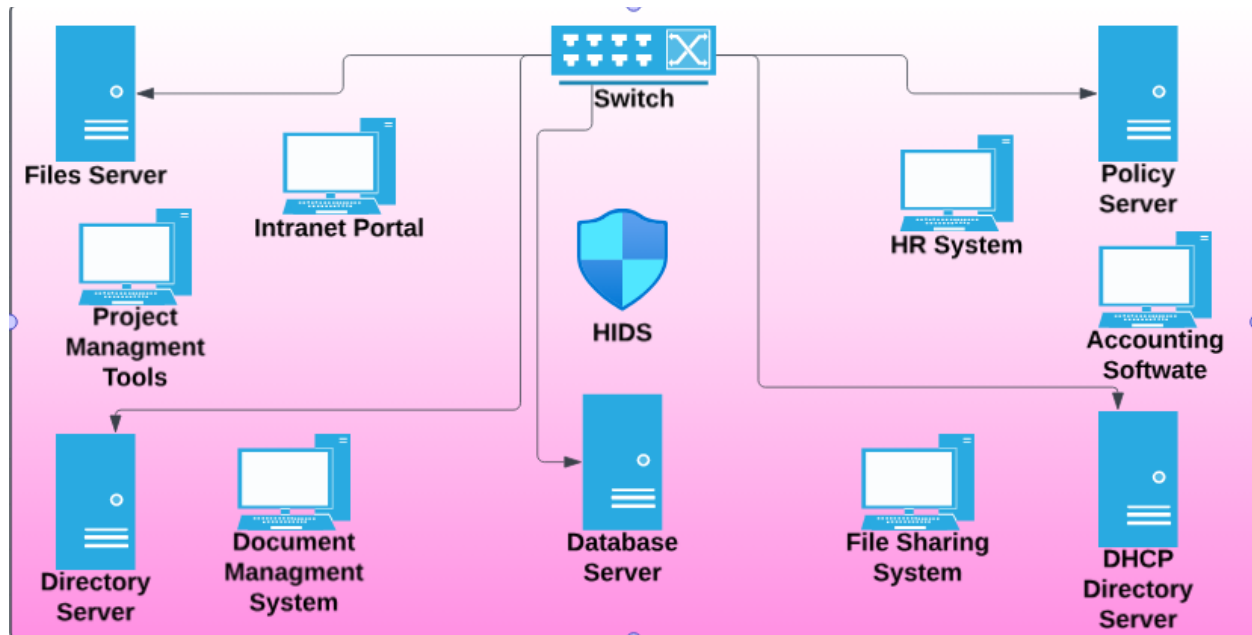
Switch: Networking device that connect multiple devices within the same network

Files Server: Servers that provide centralized storage for files and allow users within the network to share and access them

Directory Server: Servers that store and manage directory data, such as user credentials and permissions

Policy Server: enforce security policies within the network, particularly for authentication, authorization, and auditing

DHCP Directory Server: A protocol used to automatically assign IP addresses to devices on the network

Database Server: A server to store, manage, and process data it provides centralized access to databases and store critical application or business data

Intranet Portal: private, secure website system that serves as a central hub for employees

Project Managment Tools: software designed to help teams plan, organize, track, and complete projects more effectively

HR System: Centralizes and stores employee details, including contact information, job titles, department, start dates, and employment status, allowing easy access to accurate data

Accounting Software: helps businesses manage financial transactions, track income and expenses, create reports, and ensure accurate bookkeeping

HIDS: A security system that monitors activity on individual devices (hosts) to detect malicious activity or unauthorized access

Also, the Internal Network is connected to the external router as shown in the diagram I made

And to the Management Network of mine

Managment Network:
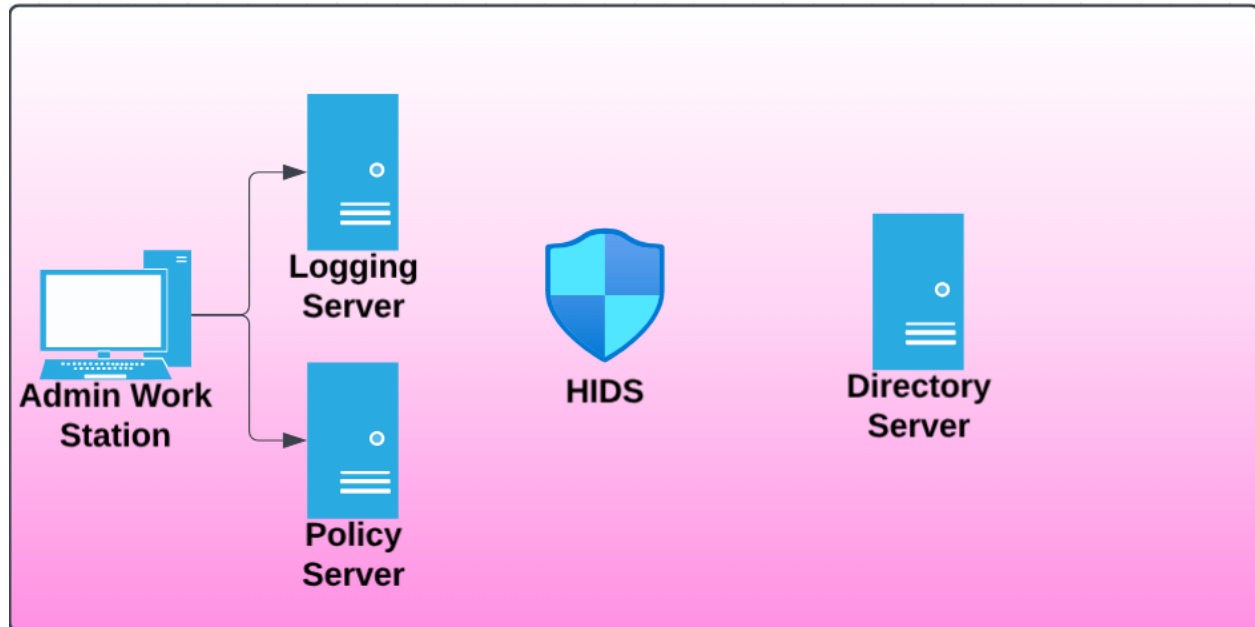
Admin Workstation: it performs critical administrative tasks, manage networks, control user permissions, and configure systems and it's isolated from the rest of the system since it can't be accessed from anyone just the owner or the admin

Logging Server: collects, stores, and manages log data from various sources across a network

Policy Server: it's the same as the policy server in the internal network but this one is more restricted and contains all the external and internal policies for the system

HIDS: A security system that monitors activity on the admin system to prevent it from any possible harmful attacks

Directory Server: stores, organizes, and manages access to directory information, such as user profiles, device information, permissions, and network resources for the system

NIDS:
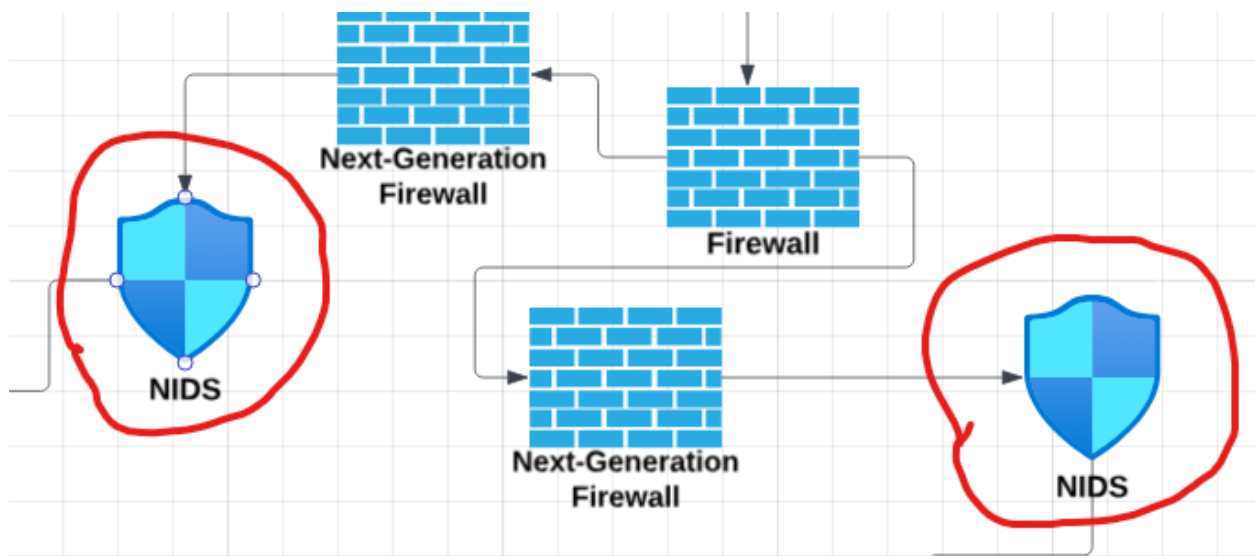
A security device or software that monitors network traffic for signs of malicious activity, such as unauthorized access or attacks, and sends alerts to administrators