Department of Artificial Intelligence and Data Science

Firewall Design Puzzle:

You are tasked with designing a firewall for a small company that has the following requirements:

1. **Internal Network Segmentation:** The company has three departments: HR, Finance, and IT. Each department should only access its own resources and the internet, but not each other's resources.

2. **Internet Access:** All departments need access to the internet, but they should not be able to access each other's internal systems.

3. **Remote Access:** The IT department requires remote access to their internal systems for maintenance purposes, but this access should be restricted to only authorized personnel.

4. **Logging and Monitoring:** All incoming and outgoing traffic should be logged for security audits.

5. **Intrusion Prevention:** The firewall should have an intrusion prevention system (IPS) to detect and block any suspicious activities.

Question:

Given these requirements, how would you configure the firewall rules? List at least five specific rules you would implement to ensure the security and functionality of the network.

Solution Example:

1. **Rule 1:** Allow all outbound traffic from HR, Finance, and IT to the internet (e.g., allow TCP/UDP 80, 443).

2. **Rule 2:** Block all internal traffic between HR, Finance, and IT (e.g., deny all traffic between the three internal subnets).

3. **Rule 3:** Allow inbound traffic for remote access to the IT department's systems only from specific IP addresses (e.g., allow TCP 22 for SSH from authorized remote IPs).

4. **Rule 4:** Log all incoming and outgoing traffic for all departments for auditing purposes.

5. **Rule 5:** Enable the IPS to monitor and block any suspicious activities across all departments.