Security hardening exercise

Part 1: Select up to three hardening tools and methods to implement
It is recommended that the organization promptly implement the following security hardening tools: firewall maintenance, multifactor authentication, and proper password policies.

Part 2: Explain your recommendations
Firewall Maintenance • The organization has to configure its network firewall with filtering rules that will only allow incoming and outgoing traffic from trusted devices. This will contribute to the enhanced security of the overall network. Multifactor Authentication • In order to protect the personal information of employees and customers alike, multifactor authentication is a must for the organization. Combining a password with at least a second form of authentication, like a one-time-only access code, will make it more difficult for threat actors to steal personal information. Password Policies • Various password policies need to be enforced by the organization. For instance, the database's admin password needs to be changed from the default to something more secure in order to guard against brute force attacks. Also, because of the threat of social engineering, employees should never share their passwords. Additionally, the organization can implement a password rotation policy that will prompt employees and customers to change their passwords every three months.