Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

1. Complex password policies
2. MFA or 2FA should be used in order to authorize.
3. Firewall rules should be reconfigured and implemented with port filtering , packet filtering etc.

Part 2: Explain your recommendations

1. Passwords are the basic and most important part of the authorization, a password should be complicated so that it cannot be guessed by the malicious actor. Also the password should not be shared with anyone as it may possibly lead to malicious activity from the compromised password account.
2. Multi factor authentication is used to verify the identity of the user requesting authentication. The user has to verify himself multiple times or at least two times in order to prove their identity. This helps in preventing the malicious requests access if the attacker somehow gets the password of the account.
3. Firewalls are the most important part of an organization's defense, as it helps in preventing the entrance of malicious packets into the organization's network. The firewall policies help in deciding which rules should be used and applied in order to maintain the access and blocking of the packets into the network.