Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
MFA Password policies Firewall maintenance

Part 2: Explain your recommendations
Implementing MFA provides an extra layer of security beyond a password. Even if one has the correct password, they still need to pass another authentication layer in order to access required account/data. This solves the problem of sharing the password amongst the employees, because the recipient of the password should possess additional authentication beside a password. Strong password policies should be implemented to strengthen the security. Policies such as suspending the account after a certain number of login attempts can help to prevent successful brute force attacks. Increasing password complexity, frequent changes of password, and not allowing password to be reused can help to prevent malicious actors from infiltrating the network. Firewall maintenance should be done regularly. Network administration should ensure that firewalls rules are up to date according to the standards for incoming and outgoing traffic. Whenever there is detection of unusual and abnormal traffic, the firewall rules should be updated in response to that event. This measure can be used to protect against various DOS and DDOS attacks.