Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The organization should implement three key security hardening methods: Multi-factor authentication (MFA) requires users to verify their identity through multiple methods, such as fingerprint scans, ID cards, pin numbers, and passwords. Strong password policies should include specific rules about password length, acceptable characters, and discourage password sharing. The policies should also address failed login attempts, such as implementing account lockouts after five unsuccessful tries. Regular firewall maintenance involves consistent review and updates of security configurations to maintain protection against emerging threats.

Part 2: Explain your recommendation(s)
MFA implementation provides security beyond traditional passwords by requiring multiple authentication methods. This approach reduces the risk of unauthorized access through brute force attacks and discourages password sharing since additional authentication factors would be needed. Comprehensive password policies make network infiltration more challenging for malicious actors. Account suspension after multiple failed attempts prevents brute force attacks, while requirements for complex passwords, regular updates, and preventing password reuse enhance overall security. Regular firewall maintenance ensures protection stays current. Network administrators should continuously update allowed and denied traffic rules, maintaining denied traffic lists for suspicious sources. Firewall rules should be updated after security incidents, particularly when suspicious traffic breaches the network, helping prevent various DoS and DDoS attacks.