# Network Hardening: Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| 1. Multifactor Authentication 2. Password Policies 3. Firewall Maintenance |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Multifactor authentication should be implemented in conjunction with strong password policies. Enforcing MFA will strongly protect against brute force attacks and ensure confidentiality, limiting access to specific assets to certain users. MFA is low maintenance, requires being implemented one time.  Password policies are paramount to protecting an organization’s assets. Creating a strong password policy will ensure users utilize alphabetical, numerical and special characters to create a secure password. Defining length and character usage will reduce the success of a brute force attack.  Firewall maintenance must be implemented because the organization does not have network traffic rules enabled. Having a firewall with properly configured rules protects against Denial of Service (DoS) attacks. This will require consistent maintenance and updating regularly. |