# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Three recommendations for implementing hardening tools or methods:   1. Port filtering 2. Multifactor authentication 3. Updating password policies |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Port filtering configuration on the firewall restricts the incoming network traffic on certain ports. This prevents any threat actors sending packets on non-standard ports and allowing this data into the network. Firewall configuration only needs to happen once during the device setup but can be updated based on business need.  Multifactor authentication adds a layer of security by having users not only authenticate using something they know, like their username and password, but also something physical like a keycard or biometric, like a retina scan. This prevents access should a threat actor guess credentials correctly. Once a policy is in place, users will not need to update their second authentication factor, but passwords may need to be changed on a cadence based on the company’s password policy.  Password policies should be updated so that they are not easily guessed. They should not be based on dictionary words and should contain capital and lowercase letters, numbers, and special characters based on the company’s security framework policy. Passwords should not be shared as certain individuals may have authorization to certain company assets that other employees do not have. This eliminates any internal potential threat to restricted company assets. Passwords should be changed on a schedule based on policy. |