

# Security risk assessment report

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

1. Firewall maintenance  
Apply firewall rules to monitor incoming and outgoing traffic. Make the firewall block all the traffics from unused ports and block IPs that try to flood servers with data
2. Multifactor authentication (MFA)  
By enforcing the use of authenticator tools, biometrics or OTPs alongside username and password to log into services
3. Password policies  
Make MFA compulsory, and discourage use of default and easy passwords

## Part 2: Explain your recommendations

Updated firewalls makes sure that rules are in place to monitor incoming and outgoing traffic and also blocks unused ports. The firewall will also prevent if someone tries to DOS the system

MFAs ensures security even if passwords get compromised due to one more step being used to log into services

Discourage password sharing and use of default passwords due to stricter password policies