Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Multi Factor Authorization (MFA) I'd implement this security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password sent to a phone number or email. Password Policies use password policies to make sure good password practices throughout the business are being followed and known. Policies can include guidelines on how complex a password should be, how often users need to update passwords, whether passwords can be reused or not, and if there are limits to how many times a user can attempt to log in before their account is suspended. Firewall Maintenance Need to add an advanced firewall that can monitor any unusual traffic on the network. Most next generation firewalls include features that detect network anomalies to make sure that oversized broadcasts or risks to systems are detected before they have a chance to bring down the network.

Part 2: Explain your recommendations
I recommend that we implement Multi Factor Authorization to strengthen user authentication, ensuring that access requires more than just a simple password. Alongside MFA, enforcing strict password policies covering complexity, update frequency, reuse limitations, and login attempt restrictions will promote best practices and reduce vulnerability. Finally, deploying advanced firewall maintenance with anomaly detection capabilities will help monitor and neutralize unusual network traffic, providing an additional layer of protection against potential threats.