Security risk assessment report

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

1. Create separate passwords for employees accessing network gear.
2. Perform an audit and remove all default passwords.
3. Explicitly deny inbound traffic, including inbound traffic from the same IP address ranges used internally.

Part 2: Explain your recommendations

1. Separate passwords for administering network gear helps to determine which users are making configuration changes.
2. Default passwords can be found online and are often used by bad actors to gain access to systems.
3. Commonly, firewalls will have an implicit deny rule from zone to zone. An explicit rule will help someone reviewing the firewall's configuration see where traffic should be limited/stopped.