o configure the firewall settings, navigate to the ‘Security’ tab in the system control panel. Select ‘Advanced Settings’ and enable ‘Inbound Rule Restrictions’. In the command line, execute: iptables -A INPUT -p tcp --dport 22 -j DROP. This will prevent unauthorized SSH access. Ensure that administrative privileges are granted before executing this command to avoid permission errors.