Planning Network Security Measures

Review the scenario and client expectations about Greenfield Properties.

Based on the information provided by the client, answer the following questions in 2-4 sentences each. Be sure to explain your answers in detail.

What types of firewall systems should be used? Explain your choice. (Ref: Firewalls Technologies and Firewalls Features and Functions)
Network Firewall with a UTM – to protect the private network from the public, it is the first line of defense for the entire network. IDS and IPS on the resource subnet where the database would reside.
What switch or router settings can be used to secure network access? Suggest one method and briefly explain its benefit. (Ref: Security Filtering - Access Control List and VPN
Port Security – closing all ports except those specifically needed for the host. On the file server shutting all incoming ports except SFTP request so port 22 will limit how many ports can be accessed and used for a malicious attack. It is an easy thing to configure that provides a multitude of protection
Which authentication method do you recommend for user sign-in to the network? Explain your recommendation. (Ref: User Authentication Methods)
Using the Kerberos method will enable the user to only have to log in once to establish their identity and then they will have access to the resources they have privileges for. This will limit the need for multiple passwords and will also increase password security because they only have the one to remember.
What password policies would you recommend enforcing? Explain your recommendation. (Ref: User Account and Password Security)
Requiring 8-15 characters at least one upper, one lower and one special character, password change every 45 days. This is the best practice for establishing a strong password.

How will the company protect physical access to the servers? Suggest two methods and briefly explain the benefits of each one. (Ref: Network Physical Security)
Servers will be locked in their own room requiring a badge. Each server rack access will be locked with a key to prevent tampering. The room should be monitored with a camera being recorded and viewed by security in another location.
What types of anti-malware software should be deployed? Explain your choice. (Ref: Anti-Malware/Anti-Virus Programs)
Cloud based anti-malware for resources in the cloud because CSP provide the most up to date security for online attacks. Utilizing Host Based Anti-Malware and Heuristic scanning for onsite hosts and resources. Host based Anti- Malware can schedule regular interval scans, schedule regular virus dictionary updates and engine will also insure we have the most up to date profiles.