1. **Discuss the three different types of firewalls (exclude circuit-level proxy).**
    - **Stateless**: Stateless firewalls filter traffic based on protocol or IP address but are less secure than stateful firewalls.
    - **Stateful**: Stateful firewalls maintain state tables, which are records of connections that are considered trusted
    - **Application Gateway**: Also called an application proxy. Acts as a relay of application-level traffic. The user contacts gateway using a TCP/IP application, the user is authenticated, and the gateway contacts application on remote host and relays TCP segments between server and user. Each application must have a proxy code. This could restrict application features that are supported. It tends to be more secure than packet filters. A disadvantage is the additional processing overhead on each connection.

2. **Discuss the SSL/TLS handshaking phases.**
    - SSL/TLS handshakes are messages exchanged by a client and a server. It has multiple steps as information is exchanged and further conversation becomes possible. A handshake is initiated when a client sends a hello message to the server. The TLS version and client random are included. Next the server will send a message with the server's SSL certificate, the server's cipher suite, and the server random. This establishes a connection and digital certificate that contains a public key. The client verifies the server's SSL and confirms the identity is correct. The client sends the premaster secret which is encrypted with the public key and can be decrypted with the server's private key. The server then decrypts the premaster secret. Next the session keys are created by both the client and the server. These are created from the server random and premaster secret. The client sends the server a message that is encrypted with the session key. The server then sends a message encrypted with a session key. Lastly the handshake is completed, and communication can continue using the session keys.