ALX Project
Web infrastructure design

Task 2.
Definitions and Explanations.

1. **For every additional element, why you are adding it:** We've fortified our infrastructure with individual firewalls for each server, securing against potential attacks. An SSL certificate now protects www.foobar.com over HTTPS, ensuring encrypted data transmission. Three monitoring clients send logs to Sumo Logic for real-time performance tracking, enabling swift issue resolution and maintaining overall system robustness.
2. **What are firewalls for:** A network security system, it monitors and controls incoming and outgoing network traffic according to predefined security rules. Essentially, it acts as a barrier, segregating a trusted network from an untrusted one.
3. **Why is the traffic served over HTTPS:** Previously, the traffic operated over Hypertext Transfer Protocol (HTTP), transmitting data in plain text. The shift to HTTPS is pivotal for security, as it encrypts data using Transport Layer Security (TLS), ensuring a secure and confidential transmission environment.
4. **What monitoring is used for:** It offers the ability to proactively detect and diagnose web application performance issues, ensuring a proactive approach to maintaining optimal functionality.
5. **How the monitoring tool is collecting data:** The system collects logs from the application server, MySQL Database, and Nginx web server. In computing, a log is an automatically generated and time-stamped documentation of events pertinent to a specific system, providing a comprehensive record for analysis and troubleshooting.
6. **Explain what to do if you want to monitor your web server QPS:** With a web server managing 1,000 queries per second (QPS), monitoring is essential on both the network and application levels. This dual approach ensures comprehensive oversight, allowing for the identification of potential issues, performance bottlenecks, and overall system health.

Issues.

1. **Why terminating SSL at the load balancer level is an issue:** The challenge arises from the resource and CPU-intensive nature of decryption. By offloading the decryption burden onto the load balancer, the server can allocate its processing power to handle application tasks efficiently.
2. **Why having only one MySQL server capable of accepting writes is an issue:** If the server is down, it implies that no data can be added or updated, leading to the non-functionality of certain features within the application.
3. **Why having servers with all the same components (database, web server and application server) might be a problem:** The vulnerability arises because if there's a bug in one component on one server, that same bug will persist across other servers.