Web infrastructure design

* For every additional element, why you are adding it

- We need SSL (Secure Sockets Layer) in a web infrastructure to encrypt communication between the web server and client devices, ensuring that sensitive information such as passwords, credit card information, and personal data are protected

- Firewalls monitor incoming and outgoing traffic, checking for suspicious activity and blocking traffic from known malicious sources.

- Monitoring tools can help to track performance metrics such as resource utilization, server response times, and error rates.

* What are firewalls for

- is a security systems that are designed to protect computer networks from unauthorized access, block malicious traffic, and prevent cyber attacks.

* Why is the traffic served over HTTPS

- to provide a secure and encrypted connection between the web server and client devices.

* What monitoring is used for

- used to track the performance, availability, and security of the system. Monitoring tools help to collect data on metrics such as CPU usage, network traffic, server response times, error rates, and security events.

* How the monitoring tool is collecting data

- it collects logs of the application server, MySQL Database and Nginx web server. A log in a computing context is the automatically produced and time-stamped documentation of events relevant to a particular system

* Explain what to do if you want to monitor your web server QPS

- If you want to monitor the QPS (queries per second) of your web server, you can use a monitoring tool such as Prometheus, Datadog, or Nagios. These tools can collect data about the requests and responses of your web server and provide metrics such as QPS, response time, and error rate.

**Issues are with this infrastructure**

* Why terminating SSL at the load balancer level is an issue

- Terminating SSL (Secure Sockets Layer) at the load balancer level can be an issue because it makes the data transmitted between the load balancer and the application servers vulnerable to interception or eavesdropping.

* Why having only one MySQL server capable of accepting writes is an issue

- Because it creates a single point of failure (SPOF) for the entire database system. If the single MySQL server goes down, the entire application may become unavailable to users

* Why having servers with all the same components (database, web server and application server) might be a problem

- If all servers have the same components, a bug in one server can affect all servers, making it a potential problem.