2. Secured and monitored web infrastructure

You must be able to explain some specifics about this infrastructure:

For every additional element, why you are adding it

3 Firewalls

Firewalls are a security technology; their role is to limit access to networks/computers. They are a division between a private network and an outer one, and they manage traffic by analyzing packets of data and allowing or blocking transfer according to user defined rules.

1 SSL certificate

Secure Sockets Layer is a protocol for encrypting communication between your application and a web browser, hence providing a safe and secure way to transmit sensitive data, including personal information, credit card details, and login credentials. It is essential for boosting security and performance.

3 Monitoring Clients

These will play a crucial role in gathering and storing data about all components of our infrastructure by keeping track of metrics, recording them and alerting if something out of the ordinary occurs; hence providing insights on infrastructure availability, reliability and performance. They will send this data to our Data Collector Sumologic.

- **What are firewalls for:** For monitoring traffic between your network and an untrusted network; and blocking or allowing data between the two based on user defined rules.

- **Why is the traffic served over HTTPS:** Previously it was served over Hypertext Transfer Protocol, which is textual hence insecure. HTTPS is a secure version of HTTP, which encrypts communication between a website and a web browser.

- **What monitoring is used for:** Monitoring gathers data about our infrastructure, which we use to keep track of our system hence detect and diagnose any issues ranging from performance to availability.

- **How the monitoring tool is collecting data:** It collects logs, traces, metadata and metrics of the Application servers, the MySQL Database and the Nginx web servers

- **Explain what to do if you want to monitor your web server QPS:**
  QPS - Queries per second
  One web server handles 1K QPS.
  To monitor, do the following:

1. Calculate the required resources based on expected QPS.
2. Monitor Server resources such as Disk, Memory and CPU Usage.
3. Then scale the server correspondingly so as to handle current and future needs.

- **Why terminating SSL at the load balancer level is an issue**
    1. If the load balancer fails, all traffic is affected. So this becomes SPOF. Can be remedied by increasing the number of load balancers.
    2. Traffic between the servers and the load balancer is not encrypted leading to data vulnerabilities.

- **Why having only one MySQL server capable of accepting writes is an issue**
  SPOF: If the Master DB fails, then all write operations fail, because it is solely responsible for these operations. Meaning data can not be updated, inserted or deleted from the database. Could lead to performance issues.

- **Why having servers with all the same components (database, web server and application server) might be a problem**
    1. If all servers have the same components then they are susceptible to the same vulnerabilities. If one component of a particular server fails, chances are it will fail for the other servers. If an attacker can access one server, chances are he can access the others as well.
    2. Since they are all identical, if updates fail for one server then they will probably fail for the others, making maintenance more challenging than if each server had diverse components.