Some specifics about this infrastructure:

Firewalls are used to protect the servers from unauthorized access and attacks. They are used to filter traffic and block any malicious traffic that may harm the servers.

HTTPS is used to encrypt the traffic between the server and the client. This ensures that any data transmitted between the two is secure and cannot be intercepted by third parties.

Monitoring is used to keep track of the server's performance and detect any issues that may arise. It is used to ensure that the server is running smoothly and that there are no issues that may affect its performance.

The monitoring tool collects data by monitoring various metrics such as CPU usage, memory usage, disk usage, network usage, etc. It then analyzes this data to detect any issues that may arise.

If you want to monitor your web server QPS (Queries Per Second), you can use a tool like Apache JMeter or Gatling. These tools allow you to simulate user traffic and measure the server's response time and QPS.

Some of the issues with this infrastructure:

Terminating SSL at the load balancer level is an issue because it exposes the unencrypted traffic between the load balancer and the web servers. This can be a security risk if there are any malicious actors on the network.

Having only one MySQL server capable of accepting writes is an issue because it creates a single point of failure. If this server goes down, then the entire website will be unavailable.

Having servers with all the same components (database, web server, and application server) might be a problem because it creates a single point of failure. If one component fails, then the entire website will be unavailable.