Explanations:

1. **What are firewalls for:** Firewalls are added to enhance security by controlling incoming and outgoing traffic. They protect the servers from unauthorized access and potential threats.

   Firewalls is a network security device that monitors network traffic, it can be understood as a division or “wall” between a private network and public network which limits and blocks network traffic based on a set of security rules in the hardware or software by analyzing data packets that request entry to the network. Additionally, firewalls are used to allow remote access to a private network through secure authentication

   We add a Firewall on arrival at each server that has an internet connection, which is a security system that monitors and controls incoming and outgoing traffic, without a firewall we could be attacked from the internet and we could be vulnerable to loss of information.

2. **Why is the traffic served over HTTPS:** HTTPS stands for HyperText Transfer Protocol Secure HTTPS ensures encrypted communication between users and the web server, safeguarding data during transmission. Traffic is served in order to bring protection by using the secure port 443, which encrypts outgoing information. Then it is more difficult to spy or get access to the site’s information.

3. **What monitoring is used for:** Monitoring clients collect data about the infrastructure's performance, availability, and potential issues. Then, monitoring not only helps to make sure to maintain high quality levels, keeping the established standards and consistency, but also to help in the continuous improvement of the resources performance.

   The way data monitoring is performed, relies on checking new data against predefined rules and metrics. If data quality anomalies are detected, an alert is sent in order to give information about the metrics and rules violation, so data can be checked

4. **How the monitoring tool is collecting data:** IT monitoring is composed of three parts:

   1) Foundation; 2) Software, and 3) Interpretation in order to function.

- **Foundation:** Are related to the infrastructure at its lowest layer of the software stack. This includes physical and virtual devices, such as servers, CPU and Vms.
- **Software:** The software is the monitoring section which analyzes what is happening in the devices (physical or virtual machines) in terms of CPU usage, load, memory, and running count.
- **Interpretation:** Here is where collected data is turned into metrics and are presented through graphs or data charts (mostly on GUI dashboard).

This is often integrated with tools of data visualization to help better understand and do data analytics of performance.

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

   Queries per second is a measure of the rate of traffic going in a particular server serving a Web domain. It is an important metric to monitor, because it can help you decide whether to scale the server in order to cope with the demand of usage, and resource requirement so the web page won't collapse in the future with overload server request.

6. **Load Balancer (HAproxy):** The load balancer distributes incoming traffic among multiple servers, enhancing performance and preventing overload on any single server.
7. **Monitoring:** Monitoring tools track server performance, resource usage, and other metrics. They help identify issues and optimize the infrastructure.
8. **Why using SSL in Load balancer level?**

   Load Balancer SSL Termination: In a load-balanced setup, SSL termination usually occurs at the load balancer. This means that the load balancer decrypts incoming HTTPS traffic and forwards it to the appropriate back-end server as HTTP traffic. The communication between the load balancer and back-end servers can be in plain HTTP.

Issues with the Infrastructure:

1. **Terminating SSL at Load Balancer:** Terminating SSL at the load balancer means SSL decryption occurs there, potentially exposing unencrypted traffic within the internal network.
2. **Single MySQL Server for Writes:** Having only one MySQL server accepting writes poses a single point of failure. If it fails, the database becomes inaccessible.
3. **Uniform Server Components:** Servers with identical components can lead to uniform vulnerabilities. A compromise in one component might affect all servers.
4. **Monitoring QPS (Queries Per Second):** To monitor web server QPS, you would configure monitoring tools to track the number of queries processed by the web server over a specific time period.