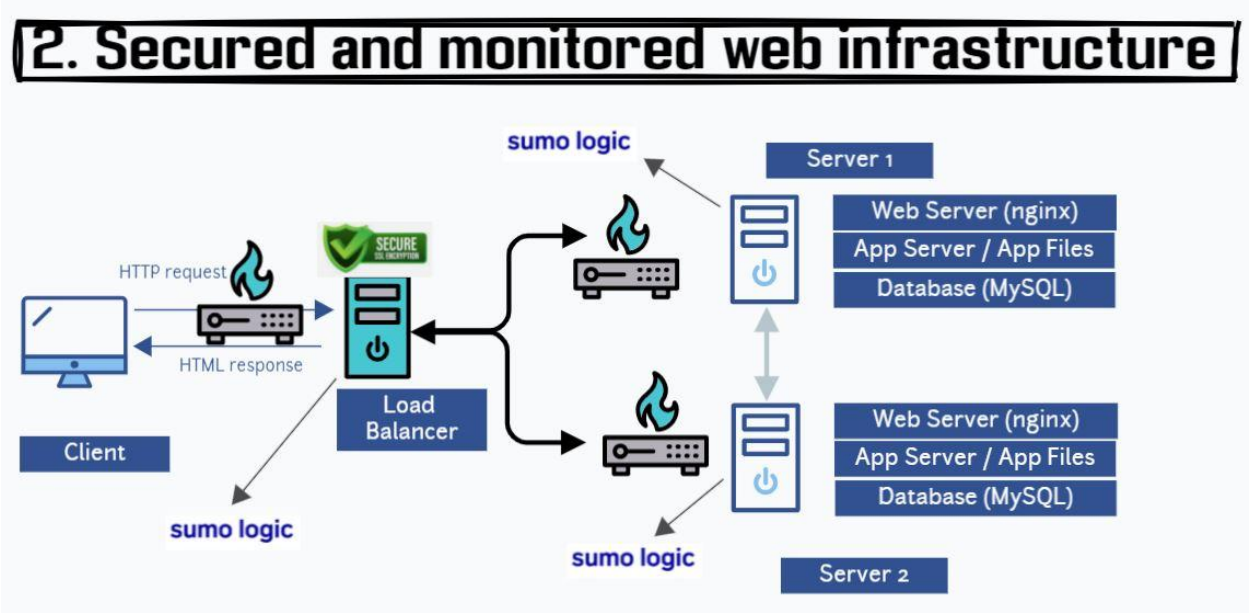

- For every additional element, why we are adding it:
    - Firewall: to protect against outside cyber attackers by shielding our network from malicious or unnecessary network traffic.
    - Monitoring: to make sure that the network is running optimally.
    - SSL certificate: to ensure our clients that their data is secure on transit.

- What are firewalls for:
  Firewalls establish a barrier between an internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

- Why is the traffic served over HTTPS:
  HTTPS uses secure port 443, encrypting information, so it is much more difficult to spy on the site data.

- What monitoring is used for:
  A monitoring system helps to increase productivity, getting key insights into server and infrastructure issues
  Monitoring devices improves the use of the hardware. If, for example, a computer or any device is not working properly, the monitoring tool will detect it, give notice of it and then, it can be repaired or replaced.

- How the monitoring tool is collecting data:
  Network monitoring systems use different protocols to collect data about the network (hardware and software) function. For example:
    - ➢ SNMP - The Simple Network Management Protocol is an application-layer protocol that uses a call-and-response system to check

statuses of many types of devices, from switches to printers. SNMP can be used to monitor system status and configuration.

- ➢ ICMP - Network devices, such as routers and servers, use the Internet Control Message Protocol to send IP-operations information and to generate error messages in the event of device failures.

- Explain what to do if you want to monitor your web server QPS:
  All traffic goes through the load balancer, so the monitoring tool there keeps track of QPS

- Why terminating SSL at the load balancer level is an issue:
  Because traffic between the load balancer and the app servers would be unencrypted. That wouldn't be so much of an issue if the load balancer were within the same data center as the web servers.

- Why having only one MySQL server capable of accepting writes is an issue:
  Because if something happens to the master server the replica may not be up to date.

- Why having servers with all the same components (database, web server and application server) might be a problem:
  Having dedicated servers is a better solution from a security perspective. For example if a hacker gains access to your web server, or if some failure of hardware or software occurs, your data may still be safe on its own server.