## Secured and monitored web infrastructure

## Specifics:

### SSL Certificate:

SSL certificates are what enable websites to use HTTPS, which is more secure than HTTP. An SSL certificate is a data file hosted in a website's origin server. SSL certificates make SSL/TLS encryption possible, and they contain the website's public key and the website's identity, along with related information.

### What are firewalls for?

A firewall is a security system designed to prevent unauthorized access to or from a private network. Firewalls can be hardware-based, software-based, or a combination of both. They are commonly used to protect corporate and home networks from external threats such as hackers, malware, and viruses. Firewalls use a set of rules to control incoming and outgoing network traffic and can be customized to fit the specific security needs of a network.

### Monitoring

A monitoring tool is a type of software or hardware that is used to collect data about a system, network, or application. This data can be used to monitor the performance and health of the system, identify potential issues, and take corrective action as needed. Monitoring tools can provide valuable insights into the behavior and operation of a system, and can help ensure that it is running smoothly and efficiently. Some common types of monitoring tools include network monitoring tools, server monitoring tools, application performance monitoring tools, and website monitoring tools. These tools can be used to monitor a wide range of metrics, including availability, latency, throughput, error rates, and more.

### Why is Traffic Served Over HTTPS?

HTTPS is a secure version of the HTTP protocol, which is the protocol used to transfer data over the web. When a website uses HTTPS, it means that all communication between the web server and the client’s web browser is encrypted and secure. This is important for a number of reasons, including protecting the privacy of users’ personal information and preventing attackers from intercepting and altering the data that is transmitted between the server and the client. Additionally, because HTTPS provides a secure connection, it helps to ensure the integrity of the data that is transmitted, which is important for ensuring that the information on a website is accurate and up-to-date.

**What to do to Monitor a Web Server's QPS:**

If you want to monitor your web server's QPS (queries per second), you can use a variety of tools to do so. Some popular tools for monitoring web server performance include:

1. **Netdata:** This is an open-source real-time performance monitoring tool that can be used to monitor a wide range of metrics, including QPS, on your web server.

2. **Datadog:** This is a cloud-based monitoring and analytics platform that can be used to monitor your web server's performance, including QPS.

3. **Prometheus:** This is an open-source monitoring and alerting toolkit that can be used to monitor your web server's QPS, as well as other metrics.

**Drawbacks:**

**Why Terminating SSL at the Load Balancer Level is an Issue:-**

Terminating SSL at the load balancer level can cause a number of issues. For one, it can create a single point of failure, since all SSL traffic has to pass through the load balancer. This means that if the load balancer goes down, SSL traffic will no longer be able to pass through, potentially causing outages on your site. Additionally, terminating SSL at the load balancer level can create performance bottlenecks, since the load balancer now has to handle the additional processing required to encrypt and decrypt all SSL traffic.

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

Having only one MySQL server that is capable of accepting writes can be problematic for a number of reasons. For one, it can create a single point of failure in your system. If that server goes down for any reason, your entire system will be unable to accept writes, which can cause significant disruption to your business. Additionally, having a single server that is responsible for accepting all writes can lead to performance bottlenecks, as the server may become overwhelmed by the volume of incoming write requests. This can cause your system to slow down or even crash.

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

Having all the same components on multiple servers can lead to potential problems if one of those components experiences an issue or fails. If a server's database, for example, goes down, it can take the rest of the system down with it. This can lead to decreased reliability and increased downtime for the system as a whole. It's generally considered a best practice to have different servers for different components to increase reliability and reduce the impact of any potential issues. This way, if one server experiences an issue, it won't take the entire system down with it.

Authors:
Lawrence Siro
Ami Choudhary