

* **For every additional element, why you are adding it**

3 Firewalls: The first Firewall checks the rules after receiving the requests and can deny the following requests. The second firewall works in the server to prevent someone from hacking depending on the requests, and the third firewall acts as circuit-level firewall, inspecting the transaction of the information.

SSL certificate: 1 SSL certificate: is added to secure HTTPS protocols and encrypt communication. Then, the ‘plain text’ won’t be easily accessed or viewed by a third person, making the protocol communication and data transfer from the browser and web server more secure (Instant SSL, 2021)

* **What are firewalls for**

A firewall is a network security device that monitors network traffic. It can be understood as a division or “wall” between a private network and a public network that 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.

* **Why is the traffic served over HTTPS**

HTTPS stands for HyperText Transfer Protocol Secure, and the traffic is served to bring protection by using the secure port 443, which encrypts outgoing information. Then it is more challenging to spy or access the site’s information.

* **What monitoring is used for**

Monitoring is a practice used for quality control. As Peter Ducker said, “What can’t be measured, it can’t be improved.” Then, monitoring not only helps to maintain high-quality levels, keeping the established standards and consistency but also to help in the continuous improvement of the performance of the resource.

* **How the monitoring tool is collecting data**

1. Foundation: These are related to the infrastructure at its lowest layer of the software stack. This includes physical and virtual devices like servers, CPUs, and VMs.
2. Software: The software is the monitoring section that analyzes what happens in the devices (physical or virtual machines) regarding CPU usage, load, memory, and running count.
3. Interpretation: Here, collected data is turned into metrics and presented through graphs or charts (mainly on the GUI dashboard). This is often integrated with data visualization tools to help better understand and do data analytics of performance (Gillis, 2020).

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

A measure of the volume of traffic flowing into a particular server handling a Web domain is the number of queries per second. It is crucial to track this measure to determine whether to scale the server to handle user demand and resource requirements and prevent future server overload web page collapse.

* **Why terminating SSL at the load balancer level is an issue**

However, such practice implies that SSL termination at the Load Balancer also poses a security risk because the data that are passing across the network from the load balancer to the App Server are now unencrypted, and that will leave applications vulnerable to Man-in-the-Middle Attack (MITM) (Boisrond, 2014).

* **Why having only one MySQL server capable of accepting writes is an issue**
* It could be more reliable because of the asynchronous replication. This means that some transactions committed by the master may not be available to the slave if the master fails.
* Write requests can hardly be scaled up. The only option to scale write requests is to increase the computational capacity (RAM and CPU) of the master node.
* The failover process is manual in a general case. You must take care of the promotion from the replica node to the master node.
* **Why having servers with all the same components (database, web server and application server) might be a problem**

Both the web server/app code and SQL Server would cache commonly requested data in memory and you're killing your cache performance by running them in the same memory space.