* By serving as a bridge between the internal and external networks and filtering incoming traffic that meets the specified criteria, firewalls guard the network—web servers in particular—from unauthorised and undesired users.
* In order to guard against valuable information being exposed by network sniffers and man-in-the-middle attacks (MITM), the SSL certificate encrypts all communication between the web servers and the external network. Identity, privacy, and integrity are guaranteed by the SSL certificates.
* The servers and the external network are being watched over by the monitoring clients. They assess the general health of the servers, examine their functionality, and notify the administrators if any of the servers are not operating at optimal levels. The monitoring tool keeps an eye on the servers and gives the admins important operational metrics. It checks the servers' accessibility automatically, gauges response times, and sounds an alarm for problems like missing or corrupt files, security breaches, and a host of other problems.

*Issues*

* Keeps the communication between the web servers and the load balancer unencrypted.
* Due to the fact that it is not scalable and may serve as the web infrastructure's single point of failure.
* Causes the components to compete with one another for server resources like CPU and memory, which can result in subpar performance and make troubleshooting more challenging. This kind of arrangement is difficult to scale.