

Secured and monitored web infrastructure

Explaining some specifics about this Infrastructure:

Firewalls (3): Firewalls protect against unauthorized access and filter traffic.

Three firewalls, one for each server, to control incoming and outgoing network traffic.

Why Firewalls: they enforce security by controlling traffic and blocking potentially malicious requests.

1 SSL certificate to serve www.foobar.com over HTTPS: SSL certificates ensure data encryption in transit.

Why is the traffic served over HTTPS: Provides data encryption and builds trust with users.

Monitoring Clients (3):

Three monitoring clients (e.g. Sumo Logic) to collect data on server performance, security and user activity.

Monitoring tools help track system health, identify issues, and ensure optimal performance.

Specifics Issues:

Terminating SSL at the Load Balancer:

Terminating SSL at the load balancer can be a security issue because decrypted data is sent to the web servers.

If the load balancer is compromised, the data could be exposed.

Single MySQL Server for Writes:

Having only one MySQL server for writes is a single point of failure. If it fails, write operations are halted, affecting the website's performance.

Identical Server Components:

Using identical components on all servers might be problematic if one of those components has a vulnerability. If that vulnerability is exploited, all servers become vulnerable.