Imagine a server with the following specs:

● 4 times Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00GHz

● 64GB of ram

● 2 tb HDD disk space

● 2 x 10Gbit/s nics

The server is used for SSL offloading and proxies around 25000 requests per second.

Please let us know which metrics are interesting to monitor in that specific case and

how would you do that? What are the challenges of monitoring this?

In this case, we should monitor below topic:

1- Hardware and resources.

2- Traffic (Inbound and outbound).

3- Events and logs from application and requesters.

4- Latency awareness.

5- SSL version.

Additional explanation:

- Since server must encryption and decryption, it's important monitor CPU and Memory usage, although it won't need so many loads.
- Monitor memory disk to prevent memory swap, it means we don't have enough memory capacity and expand it for future.
- Monitor incoming and outgoing traffic and it must approximately equal, if it doesn't equal it means we have a problem in our side and need to check.
- Monitor RX and TX errors on NICs. So if observed number of errors goes up it need check calibration of network interfaces.
- Monitor server Availability from inside and outside of the network for instance use ping command to check.

What are the challenges of monitoring?

- Since the server is single point of failure in this case, Availability is so important and need accurate monitoring.
- Monitor ongoing sessions (Outgoing and incoming), it helps it find some attacks like DDOS before SSL offloading.