

ANSWER

Since SSL Offloading server receives, decrypts and routes the traffic to defined web/application servers, CPU would be the most important part to monitor. CPU metrics to be monitored are mentioned below.

For the proxy side, getting 25000 requests per second, Network is the most important part. Let's assume that nics are configured as LACP and total bandwidth is 20Gbit/s. Basically server can serve maximum 2.5GB (2500MB) of data per second and there are 25000 requests per second. So physical network limitation allows us to 100KB of data per request per second (assume that same requests). So, the network bandwidth (saturation) became too critical. Disk stats should be monitored depending on the situation of served package size and CDN existence. If there aren't any CDN, application serves the data acting like origin and disk stats will be more critical. Utilization and mount status of disks are also critical. If server use the local storage as application's storage, disk stats should be monitored.

Following metrics are critical to monitor server used for SSL offloading and proxy:

- CPU
 - o Utilization
 - o Interrupts per core
 - o Loads (1m, 5m, 15m) per core
 - o iowait
 - o Steal Time (more necessary if the server is virtual machine)
 - o
- Memory
 - o Utilization
- Network
 - o Interfaces State Up/Down
 - o ICMP Check
 - o Interface MTUs
 - o Bandwidth Usage
 - o TCP Connection and Packege Numbers
 - o TCP Sockets (alloc,inuse,orphan,timewait)
 - o Package Drops
- Disk
 - o Disk I/O
- File System
 - o Mounted file systems (in case of unmount suddenly)
 - o File Systems Usage
- Service URL Check
 - o Healtcheck of SSL backend (servers that accept decryptred requests) application
 - o Healtcheck of SSL URL (in case of any downtime)

These metrics can be monitored via some lightweight linux commands like top, df -h, curl , iowait etc. But it is better to keep save monitoring data to the centralized systems. So, some open-source tools like Zabbix, Netdata etc.