Task 2

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?

Fist by the number of request I need to check the ack for discart any Ddos

```
server@ubuntu:~$ sudo tcpdump -X -i ens33 |grep ack
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
13:02:15.008193 IP 192.168.1.4.ssh > 192.168.1.6.62397: Flags [P.], seq 545770674:545770882, ack 1574760146, win 6149, length 208
13:02:15.058311 IP 192.168.1.6.62397 > 192.168.1.4.ssh: Flags [.], ack 208, win 4102, length 0
13:02:17.024974 IP 192.168.1.4.ssh > 192.168.1.6.62397: Flags [P.], seq 208:528, ack 1, win 6149, length 320
13:02:17.074509 IP 192.168.1.6.62397 > 192.168.1.4.ssh: Flags [.], ack 528, win 4101, length 0
13:02:18.053349 IP 192.168.1.4.ssh > 192.168.1.6.62397: Flags [P.], seq 528:832, ack 1, win 6149, length 304
13:02:18.108938 IP 192.168.1.6.62397 > 192.168.1.4.ssh: Flags [.], ack 832, win 4106, length 0
^C23 packets captured
25 packets received by filter
0 packets dropped by kernel

server@ubuntu:~$
```

We can use the tool tcptrack

```
server@ubuntu: ~
Client                  Server                  State        Idle A Speed
192.168.1.6:53951       192.168.1.4:80          RESET        0s     0 B/s
192.168.1.6:53953       192.168.1.4:80          RESET        0s     0 B/s
192.168.1.6:62397       192.168.1.4:22          ESTABLISHED  0s     10 KB/s
192.168.1.6:53952       192.168.1.4:80          RESET        0s     0 B/s
192.168.1.6:53949       192.168.1.4:80          RESET        2s     0 B/s
```

Can be complex because I need to take a part of connection and evaluate the bandwitch consumption. But depending the service some activities can be different.

Example a website for download videos is too different the traffic that a app web server.

After it we can check the processor and rand consumption, the encryption SSL can use some more of processor.

Top -w is a good tool for it.

server@ubuntu: ~

```
top - 13:08:17 up  2:57,  2 users,  load average: 0.20, 0.22, 0.09
Tasks: 286 total,   1 running, 270 sleeping,  15 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3893.3 total,   1713.2 free,    872.8 used,   1307.3 buff/cache
MiB Swap:    923.3 total,    923.3 free,      0.0 used.   2744.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   3082 server    20   0 2935508 118224  87140 S   1.0   3.0   1:17.24 kwin_x11
   3088 server    20   0 2264800 263280 137240 S   0.7   6.6   1:20.71 plasmashell
   8586 server    20   0   11992   3900   3116 R   0.7   0.1   0:00.04 top
   2761 root      20   0  282932  64596  42720 S   0.3   1.6   0:46.96 Xorg
   4730 server    20   0   14068   6048   4568 S   0.3   0.2   0:29.58 sshd
   5173 server    20   0  899944 135576  88752 S   0.3   3.4   0:30.96 kscreenlocker_g
      1 root      20   0  168480  12400   8144 S   0.0   0.3   0:07.30 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.03 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root      20   0       0      0      0 I   0.0   0.0   0:02.41 kworker/0:0-events
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.13 ksoftirqd/0
     13 root      20   0       0      0      0 I   0.0   0.0   0:06.59 rcu_sched
     14 root      rt   0       0      0      0 S   0.0   0.0   0:00.07 migration/0
     15 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     16 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     17 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     18 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     19 root      rt   0       0      0      0 S   0.0   0.0   0:00.22 migration/1
     20 root      20   0       0      0      0 S   0.0   0.0   0:00.07 ksoftirqd/1
     22 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-events_highpri
     23 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
     24 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/2
     25 root      rt   0       0      0      0 S   0.0   0.0   0:00.23 migration/2
     26 root      20   0       0      0      0 S   0.0   0.0   0:00.10 ksoftirqd/2
     28 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/2:0H-events_highpri
     29 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/3
     30 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/3
     31 root      rt   0       0      0      0 S   0.0   0.0   0:00.23 migration/3
     32 root      20   0       0      0      0 S   0.0   0.0   0:00.22 ksoftirqd/3
```

And check the filesystem for any logs problem that can fill the hard disk.

```
server@ubuntu:~$ df -v
Filesystem     1K-blocks    Used Available Use% Mounted on
udev             1941816       0   1941816   0% /dev
tmpfs             398672    1640    397032   1% /run
/dev/sda5       19992176 7361400  11592184  39% /
tmpfs            1993360       0   1993360   0% /dev/shm
tmpfs               5120       4      5116   1% /run/lock
tmpfs            1993360       0   1993360   0% /sys/fs/cgroup
/dev/sda1         523248       4    523244   1% /boot/efi
tmpfs             398672      16    398656   1% /run/user/1000
server@ubuntu:~$
```

Depending the job activity we can use some better tools like Zabbix, if it a web server we can evaluate use a load balancer like HAProxy all depend the it team