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 ENIOMB (Ethernet), capture size 262144 bytes 13:02:15.008193 IR 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 13:02:18.108393 IP 192.168.1.6.62397 > 192.168.1.4.ssh: Flags [], ack 832, win 4106, length 0 228 packets captured 25 packets captured 25 packets dropped by kernel server@ubuntu:-$
```

We can use the tool tcptrack

```
server@ubuntu: ~
```

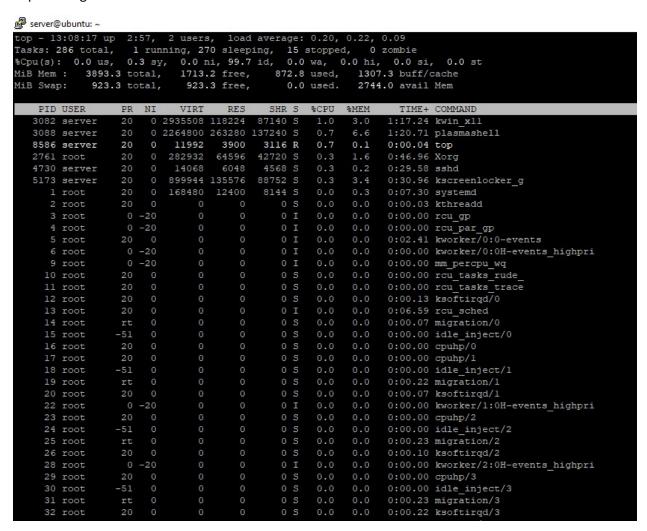
Client	Server	State	Idle A	Speed
192.168.1.6:53951	192.168.1.4:80	RESET	0s	0 B/s
192.168.1.6:53953	192.168.1.4:80	RESET	0s	0 B/s
192.168.1.6:62397	192.168.1.4:22	ESTABLISHED	0s	10 KB/s
192.168.1.6:53952	192.168.1.4:80	RESET	0s	0 B/s
192.168.1.6:53949	192.168.1.4:80	RESET	2s	0 B/s

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.



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
               1941816
                1941816 0 1941816 0% /dev
398672 1640 397032 1% /run
udev
tmpfs
/dev/sda5 19992176 7361400 11592184 39% /
tmpfs
               1993360 0 1993360 0% /dev/shm
                                          1% /run/lock
tmpfs
                   5120
                                    5116
               1993360
                            0 1993360 0% /sys/fs/cgroup
tmpfs
                523248 4 523244 1% /boot/efi
398672 16 398656 1% /run/user/1000
/dev/sdal
tmpfs
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