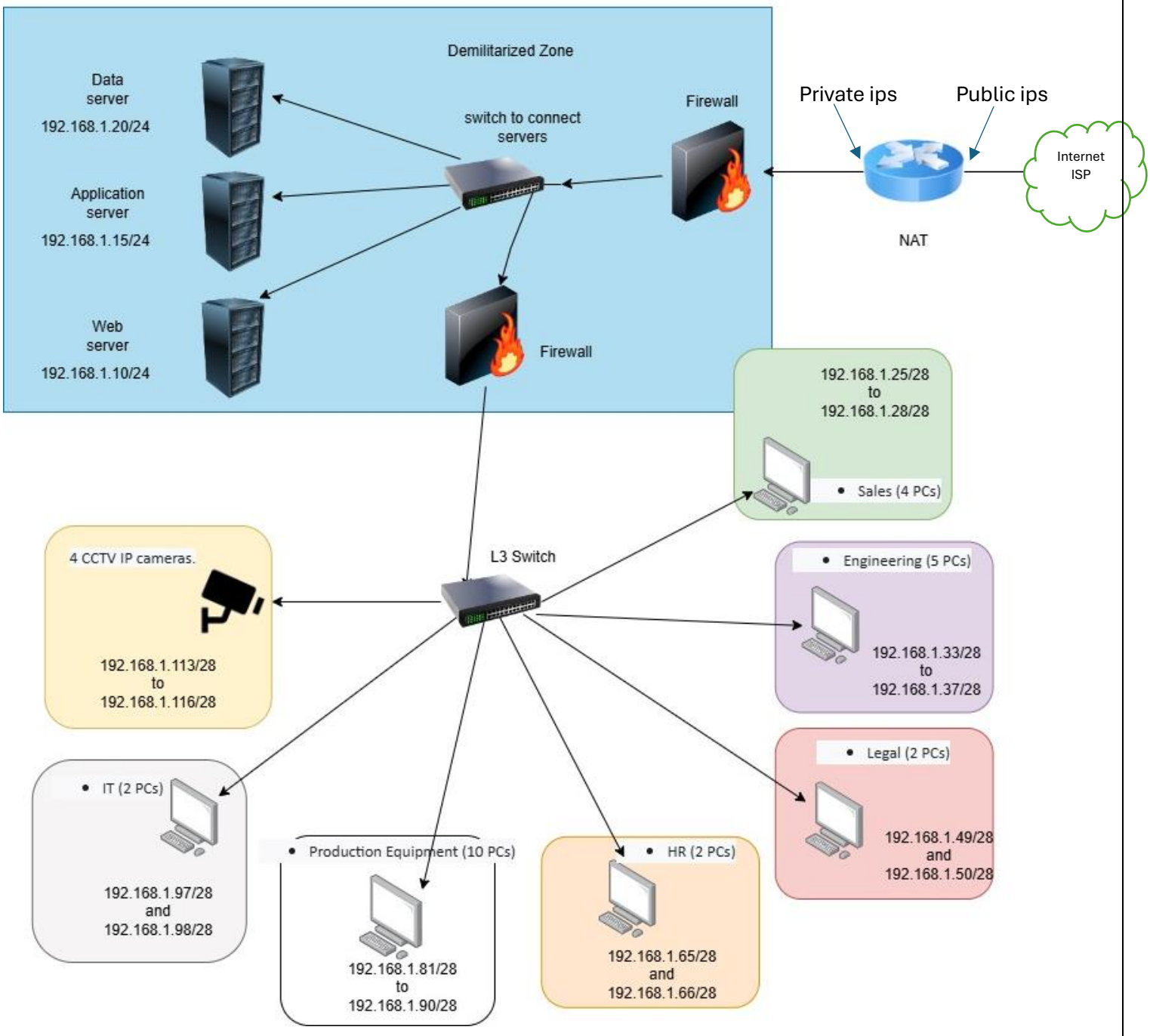
Pandora network diagram and possible improvements

Name: Lahiru Randika Index: 210527J

Diagram ;



IP Allocation Plan;

We got a full Ip portion of 192.168.1.0/24 and to keep the quality of the network; also to improve the quality of the network I made sub networks using that portion.

We have 7 divisions to represent. 7 → 8 =2^3 => 3 bits are enough. But thinkin of future growth of the network I selected /28 portion to make subnets. So we got 4 bits for our host part. That means 2^4 = 16 machines to one subnet. That can cover the PCs in subnets (max is 10 PCs). So /28 portion is selected.

192.168.1.25/28 to 192.168.1.31/28 for Sales

192.168.1.32/28 to 192.168.1.47/28 for Engineering

192.168.1.48/28 to 192.168.1.63/28 for legal

192.168.1.64/28 to 192.168.1.79/28 for HR

192.168.1.80/28 to 192.168.1.95/28 for Production

192.168.1.96/28 to 192.168.1.111/28 for IT

192.168.1.112/28 to 192.168.1.127/28 for CCTV

This can improve the quality of the network. Because of these subnetting w can apply barriers between some subnets if we want.

Additional devices ;

- Firewall: Used two firewalls to make a de-militerized zone for the servers.
- Layer 3 Switch: By considering the description, took a layer 3 switch as the core switch(48 ports) and If the network gets bigger we can use a router as a core with few switches to make subnets.
- NAT Router: To connect public ips and private ips we used an address translation router
- Access Control Devices: Can use network access control devices to enforce security policies on devices attempting to access the device
- If we want we can connect wifi routers also to make some wireless connections

Configurations and Access control rules ;

- DMZ :
    - If the data server has nothing to do with the outer world requests or it contains high sensitive data we can locate it inside the internal network (high security)
    - Allow filtered HTTP/HTTPS traffic from the outer world to the servers
    - Accept only trusted traffic from the outside (from both outer world and inner network which contains VLANs) and block other traffic using firewalls
        - Allow only the relevent traffic from IT subnet to web server in DMZ. (Web server runs on Rocky Linux 9 Server. So we can use relevent Linux protocols to handle this)

- VLANs :
    - Can use access controls within the network for security purposes
        - As an example, if there is nothing to communicate between sales and engineering we can block all the traffic between them.
        - As an example, if there is no high engagement between sales and HR we can allow only the necessary traffic and neglect the rest.
        - If CCTVs can be monitored only by HR and legal we can neglect all other unwanted traffic to CCTVs from others.
        - To achieve this we can use many techniques like access control lists, access control matrices etc.

    - Block all unwanted traffic from internal subnets to DMZ except for necessary management traffic and vice versa.

References ;

Youtube videos to get the idea on network improvements

ChatGpt to get some ideas about configurations and access control techniques