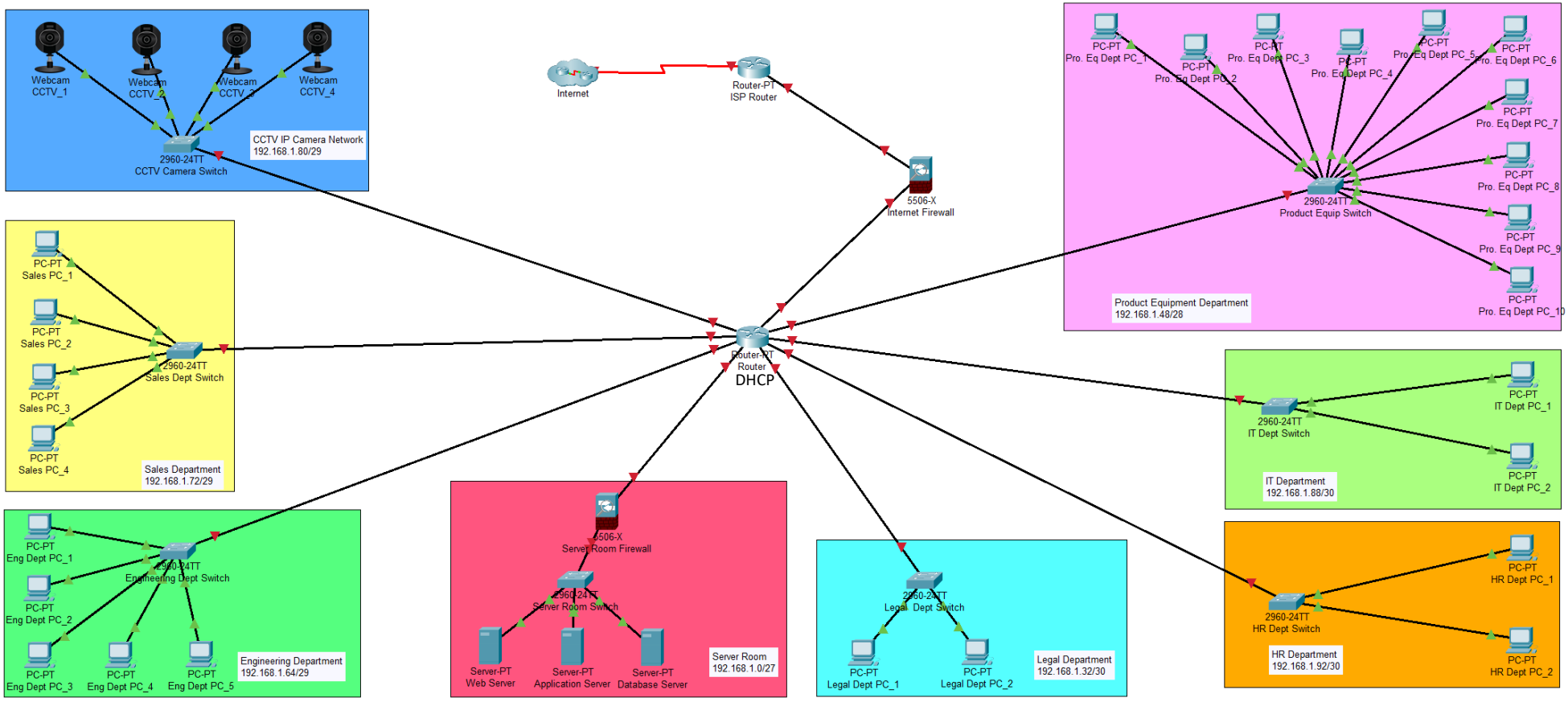
KURUKULASOORIYA KVR **200332X**

CS 3400 CYBER SECURITY PROJECT

PANDORA NETWORK DIAGRAM AND POSSIBLE IMPROVEMENTS

Network Diagram



Note : A DNS server is not included in the above diagram since the website is not yet hosted/ enabled.

Network Segmentation

Location Name		No of Devices	Network Address	Applicable Range
Server Room	**Web Server**	1	192.168.1.0/27	192.168.1.10
	Application Server	1		192.168.1.15
	Database Server	1		192.168.1.20
Legal Department		2	192.168.1.32/30	192.168.1.33 ... 192.168.1.34
Product Equipment Department		10	192.168.1.48/28	192.168.1.49 … 192.168.1.58
Engineering Department		4	192.168.1.64/29	192.168.1.65 ... 192.168.1.68
Sales Department		5	192.168.1.72/29	192.168.1.73 ... 192.168.1.77
CCTV IP Network		4	192.168.1.80/29	192.168.1.81 ... 192.168.1.84
IT Department		2	192.168.1.88/30	192.168.1.89 ... 192.168.1.90
HR Department		2	192.168.1.92/30	192.168.1.93 ... 192.168.1.94

Note: Only the 3 Servers in the Server room are configured with static IP addresses. Since other department networks are connected via DHCP configuration, the applicable pool of IP addresses for the given number of hosts is stated as above.

Firewall Rule Implementation

Assumptions:

- The web server is allowed for any external or internal incoming HTTP/HTTPS traffic. (Ports 80/443)
- IT Department has the allowed access to any device in the Pandora Network via SSH Protocol to enable remote configuration. (Port 22)
- The organization is managed using an Enterprise Resource Planning (ERP) Software and its backend system is hosted at Port 3000 in the Application Server and the front-end systems are run at Port 8000 in each PC used in each department.
- For data processing purposes, the Database Server is only allowed to access via the Application Server and it is restricted for any other direct incoming traffic. Still, the IT department is allowed access but only for the configuration purposes .
- Any other traffic other than allowed ones are denied.

1. **A Server Room Firewall is implemented to control incoming traffic :**

Source IP	Destination IP	Source Port	Destination Port	Protocol	Action
Any	192.168.1.10	Any	80	TCP	Allow
Any	192.168.1.10	Any	443	TCP	Allow
192.168.1.88/30	192.168.1.0/27	Any	22	TCP	Allow
192.168.1.0/24	192.168.1.15	8000	3000	TCP	Allow
Any	Any	Any	Any	Any	Deny

Assumptions:

- Except for Application Server, Database server, and CCTV network, all other end devices are allowed to connect to the internet and receive HTTP/HTTPS requests from incoming traffic. (Ports 80/443)

2. **An Internet Firewall is control incoming traffic :**

Source IP	Destination IP	Source Port	Destination Port	Protocol	Action
Any	192.168.1.10	Any	80	TCP	Allow
Any	192.168.1.10	Any	443	TCP	Allow
Any	192.168.1.32/30	Any	80	TCP	Allow
Any	192.168.1.32/30	Any	443	TCP	Allow
Any	192.168.1.48/28	Any	80	TCP	Allow
Any	192.168.1.48/28	Any	443	TCP	Allow
Any	192.168.1.64/29	Any	80	TCP	Allow
Any	192.168.1.64/29	Any	443	TCP	Allow
Any	192.168.1.72/29	Any	80	TCP	Allow
Any	192.168.1.72/29	Any	443	TCP	Allow
Any	192.168.1.88/30	Any	80	TCP	Allow
Any	192.168.1.88/30	Any	443	TCP	Allow
Any	192.168.1.92/30	Any	80	TCP	Allow
Any	192.168.1.92/30	Any	443	TCP	Allow
Any	Any	Any	Any	Any	Deny

Assumptions:

- Host-level firewalls are configured in each device in each department to ensure that,
  - The devices within the department's network are allowed to access each other.
  - All devices are allowed for incoming HTTP/HTTPS traffic, replies & requests from the backend hosted at the application server and also accessible to the IT department for remote configuration purposes.
  - The legal department has allowed the incoming traffic of real-time streaming of video from CCTV DVRs. (Port 37777)
  - **For the convenience of the manufacturing process, incoming FTP traffic is allowed between production Equipment with the Sales and Engineering departments.**

- Any other kind of inter-department access needs like leave mgt, order mgt, requesting services from the IT department, etc. are done via the ERP system's interface, and proper authentication/ authorization mechanisms and the least privilege-based access controls are placed in there to ensure the information security (CIA).

3. Host-level firewalls are implemented at each end device to control incoming traffic :

1. Legal Department

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.32/30	Any	Any	TCP	Allow
192.168.1.88/30	Any	22	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow
Any	Any	443	TCP	Allow
192.168.1.80/29	Any	37777	UDP	Allow
Any	Any	Any	Any	Deny

2. Product Equipment Department

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.48/30	Any	Any	TCP	Allow
192.168.1.88/30	Any	22	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow
Any	Any	443	TCP	Allow
192.168.1.64/29	20	20	TCP	Allow
192.168.1.72/29	20	20	TCP	Allow
Any	Any	Any	Any	Deny

3. **Engineering Department**

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.64/30	Any	Any	TCP	Allow
192.168.1.88/30	Any	22	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow
Any	Any	443	TCP	Allow
192.168.1.48/28	20	20	TCP	Allow
Any	Any	Any	Any	Deny

4. **Sales Department**

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.72/30	Any	Any	TCP	Allow
192.168.1.88/30	Any	22	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow
Any	Any	443	TCP	Allow
192.168.1.48/28	20	20	TCP	Allow
Any	Any	Any	Any	Deny

5. **IT Department**

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.88/30	Any	Any	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow

Any	Any	443	TCP	Allow
Any	Any	Any	Any	Deny

6. HR Department

Source IP	Source Port	Destination Port	Protocol	Action
192.168.1.92/30	Any	Any	TCP	Allow
192.168.1.88/30	Any	22	TCP	Allow
192.168.1.15	3000	8000	TCP	Allow
Any	Any	80	TCP	Allow
Any	Any	443	TCP	Allow
Any	Any	Any	Any	Deny

Note: All the traffic allowed within the network is TCP except the real-time video streaming from 4 CCTVs which is UDP.