CSA - 0735

Assignment - 5
Unit - 5

Name: G. Prashanth

Reg No: 192524.072.

a) Design firewall rules to block facebook and allow research traffic.

Priority	Source	Destination
1	Lab subnet	facebook.com.

Priority	Source	Destination	Service/Port	Action.
1	Lab subnet	facebook.com IPs	Any	Deny
2.	Lab subnet	157.240.0.0/16	Any	Deny
3.	Lab subnet	Research servers	Any	Allow
4.	Lab subnet	Internet	80/443	Allow
5.	Any	Any	Any	Deny (default)

b). ~~Total~~ Calculate total delay in packet processing.

- Rule processing time per rule : 1ms.
- Number of rules : 100

Total Delay = 100 × 1ms = 100ms per packet.

c. Recommend rule optimization techniques.

1. Place most frequently matched rules at the top.

      eg (block facebook first)

2. Combine rules using subnets instead of multiple single-IP rules

3. Use object groups (eg group all social media IPs)

4. Remove redundant or shadowed rules.

5. Implement policy-based routing for research traffic to bypass unnecessary checks.

d. Suggest logging policies for compliance.

1. Log only denied traffic to reduce storage overhead.

2. Enable logging for security-critical rules.

3. Store logs centrally using syslog or SIEM.

4. Apply log rotation and retention policies (eg keep 90 da

5. Anonymize student data for privacy compliance.