**Exercise Questions for Week 4 – Access Control and Firewalls**

E2.1.
Contrast the following AC mechanisms, Directory, Access Control List, Capability and Procedure-oriented AC, in terms of how easy it is (for each case, you should consider what the system needs to do to accomplish the operation):
i) to determine authorised access during execution.
ii) to add access for a new subject.
iii) to delete access by a subject.
iv) to create a new object to which all subjects by default have access.
v) to revoke partial rights of a subject in the system.

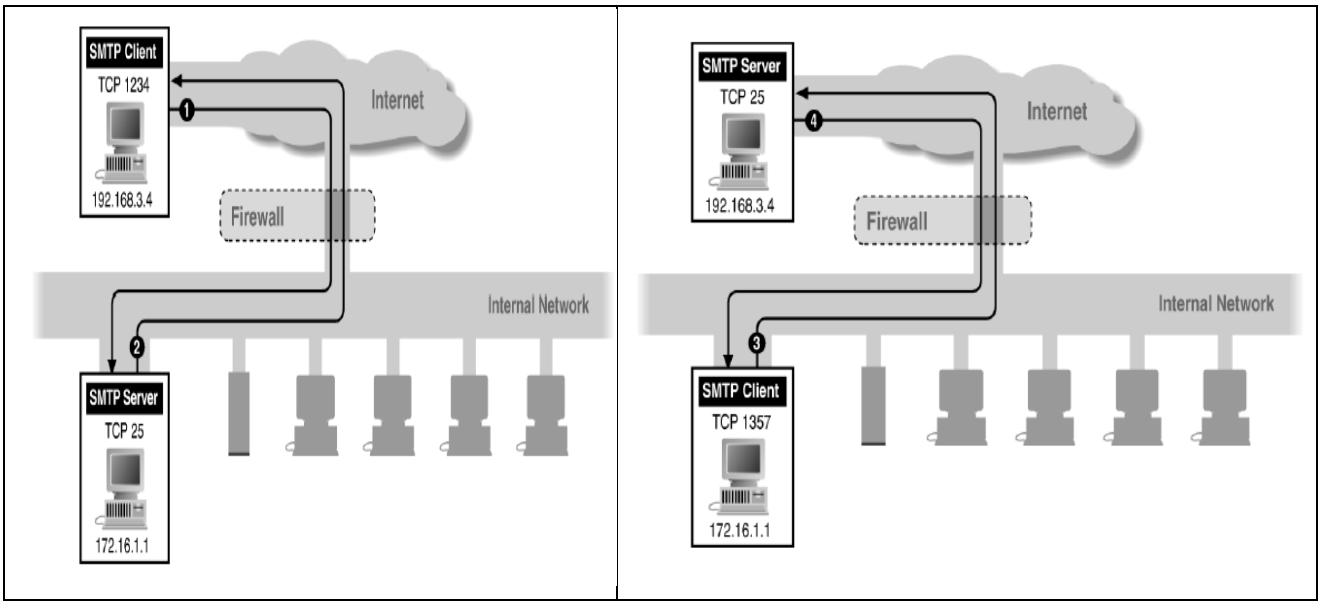
E2.2. Rewrite an AC policy using MAC to mitigate the risk of trojan horse shown in the MAC-Motivation slide.

E2.3. Suppose we have the following rule set, as shown in the table below, for a *screening* router firewall, where,

- Rules A and B allow inbound SMTP connections (incoming email), as shown in the lower-left diagram.
- Rules C and D allow outbound SMTP connections (outgoing email), as shown in the lower-right diagram.

We assume that, for each packet, your filtering system looks at the rules in order. It starts at the top until it finds a rule that matches the packet, and then it takes the action specified.

| Rule | Dir | S. Addr | D. Addr | Protocol | D. Port | Action |
|---|---|---|---|---|---|---|
| A | In | External | Internal | TCP | 25 | Permit |
| B | Out | Internal | External | TCP | >1023 | Permit |
| C | Out | Internal | External | TCP | 25 | Permit |
| D | In | External | Internal | TCP | >1023 | Permit |
| E | Either | Any | Any | Any | Any | Deny |




Answer the following questions:

(a) Imagine someone from outside (e.g. someone on host 10.1.2.3) attempts to open a connection from port 5150 on his end to the web proxy server on port 8080 on one of your internal systems (say, 172.16.3.4) in order to carry out an attack. Would this rule set be able to stop the attacking packets? Justify your answer.

(b) If the answer to question (a) is 'no', what can you do about this?

(c) Now imaging there is a smarter attacker - he uses port 25 as the client port on his end, and then attempts to open a connection to your web proxy server. Write out the rule set that could be applied to stop this attack (i.e. to filter out the attack packets)?