1. Should be in the DMZ:
   - webserver for the company' s public website (HTTP on TCP port 80)
   - mail server (SMTP on TCP port 25)

   Should be in the internal network:
   - printer server for local computers (LPR on TCP port 515)
   - fileserver storing sensitive information (SMB on TCP port 445)

Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are: Web servers, Mail servers, FTP servers, VoIP servers.

2. iptables -A FORWARD -p tcp --dport PORT --source IP --destination IP -m state --state STATES -j ACTION

1) Do not allow connections from the Internet or the DMZ to the internal network.
   - Iptables -A FORWARD -p tcp --source 203.0.113.128/25 --destination 203.0.113.128/25 -m state --state NEW, ESTABLISHED -j ACCEPT
   - iptables -A FORWARD -p tcp --destination 203.0.113.128/25 -m state --state NEW, ESTABLISHED -j DROP

2) Allow connections from the Internet to the servers in the DMZ (but only to the ports that are used by the services provided by these servers, see Problem 1), but not to any other host or port.

3) Allow connections from the internal network to the DMZ and the Internet.
   - iptables -A FORWARD -p tcp --dport 80 --destination 203.0.113.0/25 -m state --state NEW, ESTABLISHED -j ACCEPT
   - iptables -A FORWARD -p tcp --dport 25 --destination 203.0.113.0/25 -m state --state NEW, ESTABLISHED -j ACCEPT
   - iptables -A FORWARD -p tcp –source 203.0.113.128/25 -m state --state NEW, ESTABLISHED -j ACCEPT

4) Allow connections from the DMZ to the Internet.
   - iptables -A FORWARD -p tcp --source 203.0.113.0/25 -m state --state NEW, ESTABLISHED -j ACCEPT

3.

1) alert tcp $EXTERNAL_NET any -> $WEBSERVER 80 (msg:"External net try to access admin.php"; content:"admin.php"; http_url;)
2) alert tcp $HOME_NET any -> $SMTP_SERVERS 25 (msg: "Connect to an SMTP server other than the dedicated mail"; flags: A+;)

4. Tainted variables are: 1,2,4,5,6