Additional Note

- *.*.*.* is a super set of 192.*.*.*
- 192.*.*.* is a super set of 192.168.*.*
- 192.168.*.* is super set of 192.168.1.*
- 192.168.1.* is a super set of 192.168.1.1

A packet filtering rule has the following attribute: <protocol; source; source port; destination; destination port; action>

A requirement or an evidence has the following attribute: < evidence; strength value >

The actions that a packet filter rule can take are:

- ALLOW: let the packet through
- DENY: do not forward the packet

Apart from the above mentioned points, you should have default policy implemented through filtering rules so as to allow or block the packets that do not match any of the rules. The default policy can be:

- Default ALLOW: forward all the packets that do not match any of the packet filtering rules
- Default DENY: block all the packets that do not match any of the packet filtering rules

Points to remember while ordering packet filtering rules:

- If your rule set contains a block of two or more rules with the same policy action (allow or reject) that immediately follow each other, the order of the rules in that block has no functional difference to the operation of the firewall. If you are concerned about performance, you might want to put the rules that process the largest number of packets at the top of this block and the rules that process the least number of packets near the bottom of this block.
- If two consecutive rules do not have any overlapping cases in the patterns they match, they can appear in either order without affecting the operation of the firewall. As long as no two rules in the set overlap, this can be extended to a set with more than two rules.
- If two rules overlap in the patterns they match and have different policy actions, they cannot be reordered without affecting the functional operation of the firewall. Specifically, the packets in the overlapping case will have their policy changed.
- If two consecutive rules have the same policy action and one is subset of the other, the more specific rule can be discarded and the more general rule can be kept without affecting the functional operation of the firewall. One common case of this is when your default policy is, say, accept, and the last rule just before the default policy rule also has a policy of accept. This more specific rule (not the policy, of course) can be discarded.
- Your default policy always comes at the end.

Points to remember while assigning strength value to requirement or evidence:

- With each of the requirement there is a strength value attached based on your intuition (a decimal value between 0 and 1)
- Higher the strength value, more the weight-age it carries