Additional Note

To allow incoming (outside to your network, for example, allowing access to your public website) and outgoing (from your network to outside, for example, allowing users on your network to access the World Wide Web) traffic you need to consider the following:

- *.*.*.* 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
- Prefix IPs by IP
- Prefix port numbers by PORT
- For all IPs write *.*.*.* or ANY
- For all ports write * or ANY
- Each packet has a Source IP, Source port, Destination IP, and Destination Port
- To enable (disable) FTP you need to ALLOW (DENY) traffic from and to port 21
- To enable (disable) internet/web access, you need to ALLOW (DENY) traffic from or to port 80
- To enable (disable) DNS, you need to ALLOW (DENY) traffic to port 53
- To enable (disable) incoming email, you need to ALLOW (DENY) traffic from and to port 110 and 995
- To enable (disable) outgoing email, you need to ALLOW (DENY) traffic from and to port 25 and 465
- Each argument has only one claim
- Your argument network will contain multiple interconnected arguments with possibly multiple non conflicting claims

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

The actions that a policy 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 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 policy
- Default DENY: block all the packets that do not match any policy

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