- Any computer can connect to the web server on PC1;

  -d PC1 -p tcp –dport 80 -j ALLOW

- Only PC2 can connect to the SSH server on PC1;

  -s PC2 -d PC1 -p tcp –dport 22 -j ALLOW

- No computers can connect to any other servers (e.g. FTP, Email) on PC1.

  -d PC1 -p tcp –dport 1:1023 -j DROP

  -d PC1 -p udp –dport 1:1023 -j DROP

- PC1 can access servers on PC2 and PC3

  Default Policy: ACCEPT

- Any computer can connect to the web server on PC1;

  -d PC1 -p tcp –dport 80 -j ALLOW
- Only PC2 can connect to the SSH server on PC1;

  -s PC2 -d PC1 -p tcp –dport 22 -j ALLOW
- No computers can connect to any other servers (e.g. FTP, Email) on PC1.
- PC1 can access servers on PC2 and PC3

  -s PC1 -p tcp –dport 1:1023 -j ALLOW

  -d PC1 -p tcp –sport 1:1023 -j ALLOW

  (and same for udp)

  Default Policy: DROP

Summary

- Assume servers only use well-known ports
  - 1-1023
- Real-life?
  - Some servers use higher port numbers (see /etc/services)
  - Recommend:
  - Always start with default policy DROP
  - Use Stateful Packet Inspection
    - If first packet of connection is allowed, then all subsequent packets belonging to that connection are allowed
    - Use - -state option in iptables