Firewalls: Question 1

- Let's have a firewall (*iptables*) that protects an internal company network 141.9.7.0/24
- The firewall has the following INPUT chain filter rules:

	srcip	dstip	srcport	dstport	protocol	action
1	142.5.0.0/16	141.9.7.111	*	80,443	tcp	drop
2	152.4.8.0/30	141.9.7.53	*	53	udp	accept
3	152.4.8.0/30	*	*	*	icmp	accept
4	152.4.8.9	*	*	22	tcp	accept
5	*	141.9.7.111	*	80,443	tcp	accept
6	141.9.0.0/16	141.9.7.11	*	80,443	tcp	accept
7	all	*	*	*	*	drop

Firewalls: Question 1 A

- Decide, which incoming packets will be accepted, and which will be dropped. Specify, which rule will accept/drop each packet.
  1. src: 142.8.5.11, dst: 141.9.7.11:22, tcp
  2. src: 152.4.8.2, dst: 141.9.7.12, icmp
  3. src: 142.5.17.99, dst: 141.9.7.111:443, tcp
  4. src: 141.9.7.215, dst: 141.9.7.11:443, tcp
  5. src: 2003:4860:4860::8844, dst: 2016:837:62f::b8, dstport: 53, udp

Firewalls: Question 1 B

- One of the packets from question 1 A is malicious
  - Which one?
  - What's malicious about it?
  - Add a rule that would block such malicious packets
  - In which place will you add the new rule to the table?