

12.1 Question 1

12.1.A Decide, which incoming packets will be accepted, and which will be dropped. Specify, which rule will accept/drop each packet.

- src: 142.8.5.11, dst: 141.9.7.11:22, tcp
dropped, Rule 7
- src: 152.4.8.2, dst: 141.9.7.12, icmp
accepted, Rule 3
- src: 142.5.17.99, dst: 141.9.7.111:443, tcp
dropped, Rule 1
- src: 141.9.7.215, dst: 141.9.7.11:443, tcp
accepted, Rule 6
- src: 2003:4860:4860::8844, dst: 2016:837:62f::b8, dstport: 53, udp
As IPv6 packets are not handled at all by generic *iptables* this packet is just **accepted**.

12.1.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?