# Firewall



17.1. (1 point) What is `netfilter` and what are its benefits?

17.2. (5 points) What are the five `netfilter` hooks for IPv4? What are their purposes?

17.3. (1 point) Why do we need to build a kernel module in order to use the `netfilter` hooks?

17.4. (2 points) Based on the `netfilter` diagram (can be found in the book), please describe which filter is best for enforcing the following rules:

- Restricting what comes into a computer
- Restricting what goes out of a computer

17.5. (2 points) Other than being used to implement firewalls to block packets, can `netfilter` be used to modify packets? What are the other applications of `netfilter`?

17.6. (4 points) What are the benefits of stateful firewalls that support connection-based firewall rules? Please use examples to illustrate the benefit.

17.7. (1 point) The UDP and ICMP protocols are not connection-based protocols, how do firewalls know whether a UDP or ICMP packet is part of an existing "connection"?

17.8. (2 points) Add a rule in iptables to accept packets from a trusted network `192.168.10.0/24`

17.9. (2 points) A machine has an IP address `10.0.20.5`. On this machine, you need to block incoming connections to its ports 22, 23, 80, and 443. What will you do?

17.10. (5 points) A TCP server is running on a remote machine called `sirius` using "`nc -lv 9090`". This machine is on a planet outside the Solar system. An alien named Alice living on the Earth wants to communicate with the TCP server on `sirius`, but unfortunately, the Earth has a firewall that prevents all computers on the Earth from accessing any machine outside the Solar system. Alice does have a computer on Mars, which does not have such a restrict firewall rule. Alice's computer on Mars is called `mars`, and her account name is called `alien`. (1) Please describe how Alice can use an SSH tunnel to bypass Earth's firewall, so she can talk to `sirius`. (2) Without the firewall, if Alice wants to communicate with the TCP server on `sirius`, she can use the "`nc sirius 9090`" command. Now, with the SSH tunnel and the firewall, what command should Alice run to access the server?

17.11. (3 points) This problem is based on Problem 17.10. After Alice has established an SSH tunnel between her local computer `earth` and `mars`, she can use the `nc` command to communicate with the `netcat` server on `sirius`. Please describe how the TCP packets flow, from the `netcat` client program to the destination `netcat` server.