Q1: “sudo ufw default deny incoming” sets firewall to deny by default. To allow communication with the internal network, two other rules were written, using the “ufw” commands.

Q2: The difference is that deny will only drop the incoming packets, whereas reject will return an error message to the sender. The difference is that, a deny will let the sender wait whereas the reject will tell the sender that the packet was rejected.

Q3: The clients can be reached from anywhere, which is convenient if a user tends to use different computers do manage their files. A disadvantage could be that the connection could be attacked, leaving passphrases vulnerable.

Q4: When trying to implement this, the tests were done by sending packets through the firewall to the host in the outside network. The packets were indeed blocked on the way to the inside network. However, to my disappointment, they were also blocked on the way to the outside network. They successfully reached the firewall, but did not continue from there.

Q5-Q6: By using the telnet, and netcat commands, the connections can be tested to make sure that the different connections work or are blocked by the firewall. The connections can be followed through the firewalls two interfaces, and then further onto the receiver. These connections were tested, but worked in some cases only. Therefore, I was not satisfied with the results here, but am still delivering my work.