1 Firewall Implementation

For each of the following scenarios write the appropriate iptables rules to enforce the policy statement. Test your rules and log appropriately!!!

1.1 Scenario 1: Server management

You are managing a server with a local firewall. This server should accept http and https connections from all hosts, but ssh only from a configurable ip address. In addition, the maximum number of new incoming tcp connections should be limited to 1 per second, with a burst of 10. Log all dropped and limited packets with appropriate log messages.

We will test these on your workstations next session. Make sure this works on a VM in virtualbox on your praktikum PC before next session!

1.2 Scenario 2: Honeynet firewall (graded)

According to the policy discussed in class and posted on the website, implement firewall rules to enforce this policy. Create a script that will apply these rules. Log and comment the specific rules for which you might use the QUEUE target.