For this programming assignment we were tasked with writing a firewall with the specific rules from the assignment steps.

1. Flush and delete all previously defined rules and chains

2. Write a rule that only accepts packets that originate from f1.com.

3. For all outgoing packets, change their source IP address to your own machine’s IP address (Hint: Refer to the MASQUERADE target in the nat table).

4. Write a rule to protect yourself against indiscriminate and nonstop scanning of ports on your machine.

5. Write a rule to protect yourself from a SYN-flood Attack by limiting the number of incoming ’new connection’ requests to 1 per second once your machine has reached 500 requests. 2

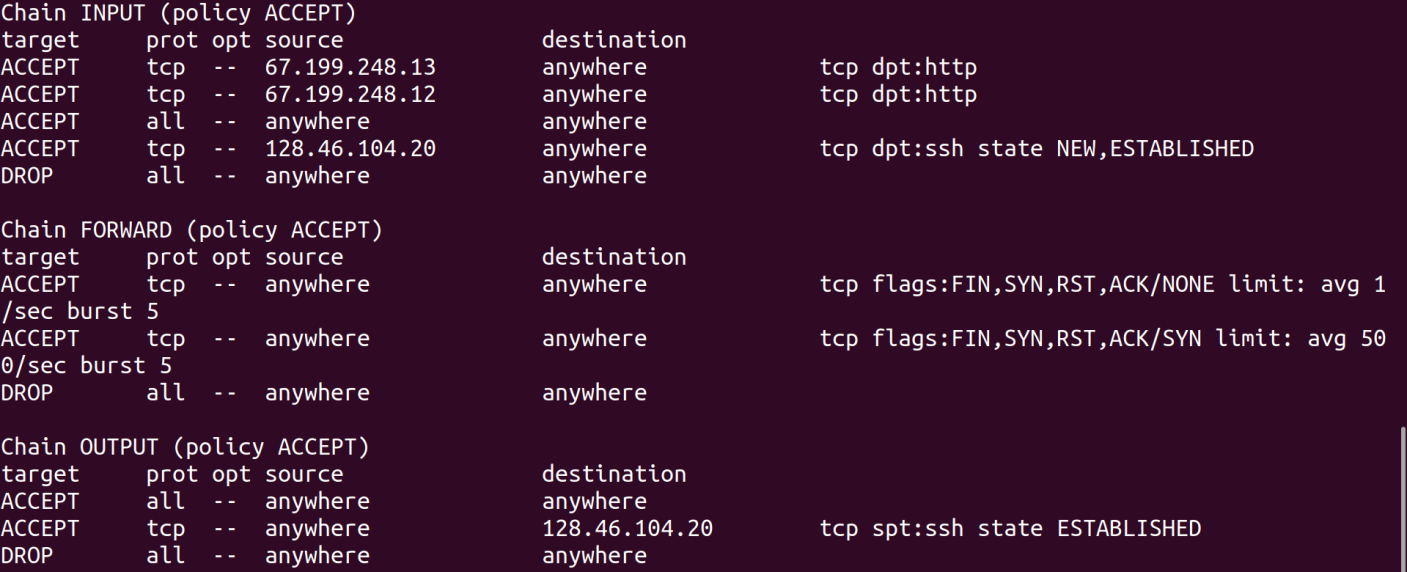
6. Write a rule to allow full loopback access on your machine i.e. access using localhost (

7. Write a port forwarding rule that routes all traffic arriving on port 8888 to port 25565

8. Write a rule that only allows outgoing ssh connections to engineering.purdue.edu.

9. Drop any other packets if they are not caught by the above rules.

We then get the firewall output from f1.com as such:



In this step we setup a spam filter and we test it by subscribing to several newsletters for spam

A screenshot of a computer

Description automatically generated