**CNLAB Report**

Team 8  
B07902002 連崇安 B07902034 王昱凱 B07902126 謝宗儒

* Environment :  
  We use Mac OS as the testing environment and use JavaScript and HTML as coding language.
* Describe how packets go through the iptables :  
  If a packet is not destined to the local machine itself, it will be routed through the FORWARD chain. If the packet is, on the other hand, destined for an IP address that the local machine is listening to, we would send the packet through the INPUT chain to the local machine.
* Describe how your program (server & webpage) interact with the iptables :  
  Webpage is the main chain in the iptables which receive and deliver packets, and determine how to deal with them (ex. send to local process).  
  Server is worked as local process in the iptables, which get input data from the FORWARD bifurcation and give output data to POSTROUTING chain.
* Your website is working on port 8080 and can only be accessed by 140.112.0.0/16. How to modify your iptables to block unavailable users?

$ iptables -A INPUT -p tcp -s 140.112.0.0/16 --dport 8080 -j ACCEPT

$ iptables -A INPUT -p udp -s 140.112.0.0/16 --dport 8080 -j ACCEPT

$ iptables -A OUTPUT -p tcp -d 140.112.0.0/16 --sport 8080 -j ACCEPT

$ iptables -A OUTPUT -p udp -d 140.112.0.0/16 --sport 8080 -j ACCEPT

$ iptables -P INPUT DROP

$ iptables -P OUTPUT DROP

* Behind the machine, there is a sshserver which locates at 192.168.10.2 in the eth1. People who want to connect to sshserver from eth0 need to connect the machine at port 2222 and the machine will redirect the flow to the sshserver at port 22.How to configure the iptable?

$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2222 -j DNAT \

--to-destination `192.168.10.2:22`

$ iptables -t nat -A POSTROUTING -o eth1 -p tcp --dport 22 -j SNAT \

--to-source `192.168.10.2`