# Solutions iptables practical sheet

1. **Set the default policy – block all input**

*iptables -P INPUT DROP*

1. **Enable loopback (ping localhost to test)**

*iptables -A INPUT -i lo -j ACCEPT*

1. **Enable ICMP (ping)**

*iptables -A OUTPUT -p ICMP --icmp-type echo-reply -j ACCEPT*

1. **Block DNS**

*iptables -A OUTPUT -p udp -o eth0 - -dport 53 -j DROP*

1. **Block outbound web access (both HTTP & HTTPS)**

*iptables -A OUTPUT -p tcp - -dport 80 - j DROP*

*iptables -A OUTPUT -p tcp - -dport 443 - j DROP*

1. **Block web access to www.wit.ie and some other website of your choice**

nslookup [www.wit.ie](http://www.wit.ie)

*iptables -A OUTPUT -p tcp - -dport 80 -d 10.5.0.56 -j DROP*

nslookup www.play.com

*iptables -A OUTPUT -p tcp - -dport 80 -d* 213.167.82.124*-j DROP*

1. **Add an ACCEPT rule. Add a conflicting REJECT rule. Which takes precedence?**

Whichever rule is added first will be matched first. Rules at the top of the chain take precedence.