# Firewall Configuration using iptables

*iptables* is a program that allows the system administrator to configure filtering rules on network interfaces of a Linux system.

## Packet Processing in iptables

All packets inspected by iptables pass through a sequence of built-in tables (queues) for processing. Each of these queues is dedicated to a particular type of packet activity and is controlled by an associated packet transformation/filtering chain.

There are three tables in total. The first is the mangle table which is responsible for dealing with the TCP header. The third table is the nat queue which is responsible for network address translation. Our focus in this practical will be on the second table, the filter queue which is responsible for packet filtering. It has three built-in chains in which you can place your firewall policy rules. These are the:

* Forward chain: Filters packets to servers protected by the firewall.
* Input chain: Filters packets destined for the firewall.
* Output chain: Filters packets originating from the firewall.

## Online Help

Help with Linux commands (options, arguments, etc) are provided using so-called “man” pages. To get help on iptables, type:

*man iptables*

A simple Google search for *man iptables* provides similar results in a web browser (which might be easier to navigate). You should familiarise yourself with the structure of *iptables* and how policies and rules are set. Some useful “How to” information can be found on the Ubuntu website.

## Practice Commands

You need to have administrator access to run the following commands. You can do this either prefacing all commands with “sudo” or logging in as the root (admin) user with the command: *sudo su.* For all the command you attempt remember to perform a test ***before*** you implement the rule and again ***afterwards*** so that you can clearly understand the operation of the rule.

**List the current configuration:**

*iptables –vL*

**Flush out the contents of the chains:**

*iptables –F*

**Simple Example: ping blocking**

1. Check connectivity to localhost: *ping localhost*
2. Then execute the following: *iptables –A OUTPUT –p ICMP --icmp-type echo-reply –j DROP*
3. Ping again, what happens?

**Remove a specific iptables rule:**

1. View current rules by line number: *iptables --line-numbers –L OUTPUT*
2. Using the line number remove the line number: *iptables –D OUTPUT <linenumber>*

**Save the Firewall configuration to a file:**

1. Export the configuration to a file : *iptables-save > firewall-config*
2. Show the contents of that file:  *cat firewall-config*

**Allow http access from the firewall to a given site x.x.x.x. (browser to test)**

*iptables –A OUTPUT –p tcp - -dport 80 –d x.x.x.x –j ACCEPT*

**Block http access from the firewall to the world:**

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

**Set the default policy – block all output**

*iptables –P OUTPUT DROP*

**Block http access to the firewall from a malicious site x.x.x.x (assuming a web server is running on the OS also) (browser to test)**

*iptables –A INPUT –p tcp --dport 80 -s x.x.x.x –j DROP*

**Block all input from a malicious site x.x.x.x**

*iptables –A INPUT –s x.x.x.x –j DROP*

## More Commands

1. Set default policies (specifically block all input by default)
2. Enable loopback (loopback address is 127.0.0.1)
3. Enable ICMP (ping)
4. Block DNS
5. Allow outbound web access (both HTTP & HTTPS)
6. Block web access to www.wit.ie and some other website of your choice
7. Add an ACCEPT rule. Add a conflicting REJECT rule. Which takes precedence?