**Linux Firewalls**

**All modern Linux kernels use the net filter system as firewall solution for packet filtering**

Netfilter needs a UI – Iptables is one interface

When a packet reaches a device, the netfilter subsystem will accept, reject or manipulate it based on the rules supplied to it by ip tables

* IP tables is all that’s necessary to manage the firewall

Ip tables allows configuration for allowing specific traffic to pass in and out or restrict or allow traffic from certain ips or ranges

* Done by closing TCP and UDP ports in the firewall
* Ip tables is the database for the firewall rules
* The UI for Iptables is the command line

Iptables -L

Shows all chains

* Input, forward and output

**Input chain** controls inbound connections

* An input rule can be specified to allow such things like people being able to ping your device
* External connections for file shares

**Forward chain** controls inbound connections as well but for those that are going to be forwarded on to a different device

* Like a router routing traffic
* Unless the device is a router or using NAT or doing something like SSL stripping then this wouldn’t be necessary on a regular computer

**Output chain** controls the outbound connections

* Wanted the laptop to surf the web, enable specific ports i.e., 53, 80, 443

IPv6 and IPv4 rules will need to be configure separately

Github.com/meetrp/personalfirewall for a guide on what rules to set

Frozentux.net/iptables-tutorial

**The policy:** drop means that if the set of rules that the connection has to follow aren’t met, then the connection will be dropped

There are 3 policy options:

* Drop
* Accept
* Reject

Iptables -F will delete all existing rules

‘Iptables -P INPUT DROP’/ACCEPT/REJECT

To set rules

**Uncomplicated Firewall (UFW)**

* Simplified (G)UI front end for iptables to make life easier
* Apt-get install UFW

**GUFW**

**Nftables –** project looking to replace ip,ip6,eb,arp tables

These are not application ware, level 4 and below

**Linux-Firewall** is an application-level firewall for Linux

Arptables

**Is it worth having a host-based firewall on a Linux laptop?**

* Linux attracts least amount of attackers
* Firewalls offer limited protection for malware that has already infiltrated the system
* Depends on what you use it for
  + Do you have untrusted devices on your network?
  + Using a hotspot or travelling