**MacOS Firewall**

System preferences 🡪 security privacy🡪 firewall🡪 **switch on**

Firewall options 🡪 V limited options

* No ability to monitor or block outgoing connections (v poor)
* Only worried about blocking incoming connections

**Command line**

‘Sudo launchctl load /System/Library/LaunchAgents/com.apple.alf.useragent.plist’

Launches the application firewall

**Packet Filter (PF) Firewall**

Comparable to iptables but for BSD and OSX

**Works only at the network and transport layer**

‘sudo nano /etc/pf.comf’ shows how pf works

Anchors: collection of rules and tables

‘pf ctl’ is main command

-sr wil show the set of rules

-ss will show current state table

-si will show filter stats and counters

-sa will show everything

-f deletes rules

-e enables firewall

-d disables firewall

Krypted cheat sheet or OS X PF manual

**GUI**

* PFLists
* IceFloor (full front-end)
* Murus Lite
* Little Snitch
  + Application based firewall
  + Easier interface
  + Live traffic monitoring

Is it worth having a host-based firewall on Mac?

* OSX is exposed to a relatively small number of malware and attacks
* However, this number is definitely on the rise
* All outbound connections are allowed
* In-built firewall on OSX has no protection against malwares creating a reverse shell and this cannot be changed without an application firewall
* Pf still only offers limited protection for compromised devices as the firewall can still be bypassed by using outbound ports that are allowed like 80 etc.
* Little snitch is better at preventing malware form communicating out