

Some Basic IPFW Rules to get you Started

This should cover basic IPFW rules. It will be enough to get your server running. This doesn't allow things like MySQL or Melange chat server. This is a default deny setup so users cant run cgi or anything to bind shells and nasty things like that. If a user wants to run a service, they have to run it by you as the admin first. The comment above each rule or set will explain it.

```
#allow everything over loopback
add allow ip from any to any in via lo0
add allow ip from any to any out via lo0
#allow some icmp so your server still pings
add allow icmp from any to any icmptypes 0,3,8,11,12,13,14
#allow ftp
add allow tcp from any to any 21 in via xl0 setup
#allow ssh
add allow tcp from any to any 22 in via xl0 setup
#allow smtp
add allow tcp from any to any 25 in via xl0 setup
#allow my dns server to be quired
add allow udp from any to any 53 in via xl0
add allow udp from any 53 to any out via xl0
#some highly loaded dns servers may need tcp aswell, and also for zone transfers
add allow tcp from any to any 53 in via xl0 setup
#allow my server to query the server in /etc/resolv.conf, this rule is dependant on what you have in /etc/resolv.
conf which should be your datacenters DNS server
add allow udp from any to 69.90.250.18 out via xl0
add allow udp from 69.90.250.18 to any in via xl0
#allow httpd(apache)
add allow tcp from any to any 80 in via xl0 setup
#allow pop3
add allow tcp from any to any 110 in via xl0 setup
#allow imap
add allow tcp from any to any 143 in via xl0 setup
#allow https
add allow tcp from any to any 443 in via xl0 setup
#allow smtps
add allow tcp from any to any 993 in via xl0 setup
#allow pop3s
add allow tcp from any to any 995 in via xl0 setup
#allow outbound setup connections
add allow tcp from any to any out via fxp0 setup
#allow in and outbound established connections
add allow tcp from any to any out via fxp0 established
add allow tcp from any to any in via fxp0 established
#deny and log everything else
add deny log logamount 1000 all from any to any in via xl0
#Only log 1000 lines, this is incase of DDoS so your machine is not taken down by logging packets it's block-
ing
```