

# Linux and PF firewalls commands cheat sheet

## Firewalld daemon management (Red Hat based distributions)

Table 1. firewall-cmd commands

Command	Description
<b>firewall-cmd --state</b>	Show firewall daemon status
<b>firewall-cmd --list-all</b>	List currently active rules
<b>firewall-cmd --reload</b>	Reload firewall keeping the state table. Active sessions do not disconnect. On finishing reload will output <b>success</b> .
<b>firewall-cmd --get-default-zone</b>	Show the default zone for interfaces.
<b>firewall-cmd --get-zones</b>	List all available zones
<b>firewall-cmd --get-active-zones</b>	Show active zones, including to which zone each interface belongs.
<b>firewall-cmd --list-all-zones</b>	List all zones with their rules and associated interfaces.
<b>firewall-cmd -add-service &lt;service name&gt;</b>	Add predefined service by name to the default zone, with action ACCEPT, e.g. <b>firewall-cmd -add -service ftp</b> .

## Ubuntu Uncomplicated Firewall (ufw)

Table 2. ufw management commands

Command	Description
<b>ufw status</b>	Show whether the firewall is on and if on, list the active rules.
<b>ufw enable</b>	Enable firewall.
<b>ufw disable</b>	Disable firewall
<b>ufw reload</b>	Reload firewall and rules.
<b>ufw allow &lt;predefined service name&gt;</b>	Allow some service in any direction from/to any IP address using so called <b>simple</b> rule syntax. The service names are as per <b>/etc/services</b> . E.g. to allow ssh from any: <b>ufw allow ssh</b> .

Command	Description
<code>/etc/ufw/before.rule</code>	Some rules are pre-allowed by default, to change them edit this file and reload the firewall.

## PF (Packet Filter) management for FreeBSD & OpenBSD

Command	Description
<code>pfctl -d</code>	Disable PF in place, does not survive reboot.
<code>pfctl -ef /etc/pf.conf</code>	Enable PF and load the rule set from file <code>/etc/pf.conf</code> in one go.
<code>pfctl -nf /etc/pf.conf</code>	Parse security rules soterd in a file without installing them (dry run).
<b>pass in quick on egress from 62.13.77.141 to any</b>	'Quick' rule (means allows this traffic on all interfaces, otherwise we would need 2nd rule allowing this traffic in <i>outgoing</i> direction on egress interface) to allow incoming ANY port/protocol with the source being <code>62.13.77.141</code> and destination being ANY IP address behind the PF firewall. NOTE: here, <code>egress</code> is not a direction, but a group name to which the interface in question ( <code>em0</code> ) belongs to. In OpenBSD you set it in a file <code>/etc/hostname.em0: group egress</code> .