

# PF firewall (FreeBSD, OpenBSD) configuration and debug commands cheat sheet

Author: Yuri Slobodyanyuk, <https://www.linkedin.com/in/yurislobodyanyuk/>

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

Command	Description
<b>pfctl -d</b>	Disable PF in place, does not survive reboot.
<b>pfctl -ef /etc/pf.conf</b>	Enable PF and load the rule set from file <b>/etc/pf.conf</b> in one go.
<b>pfctl -nf /etc/pf.conf</b>	Parse security rules stored in a file without installing them (dry run).
<b>pfctl -F &lt;all/rules/nat/states&gt;</b>	Flush, accordingly: <ul style="list-style-type: none"><li>• <b>all</b> Everything (filter rules, nat, but NOT stateful table - those already connected will stay so). Blank/flushed rules mean "permit any any".</li><li>• <b>rules</b> Rules only (stateful table of existing connections stay intact)</li><li>• <b>nat</b> NAT rules only</li><li>• <b>states</b> Stateful table (but again - active connections stay alive)</li></ul>
<b>pfctl -k &lt;source IP of connection to clear&gt; [-k &lt;destination&gt;]</b>	Kill an active connection from the state table. You can specify IP address as the 1st selector to the 1st <b>-k</b> and optionally, destination selector with another <b>-k</b> key. <b>0.0.0.0/0</b> as a wildcard can be used. E.g. to clear all connections from any to 10.10.10.13/32 <b>pfctl -k 0.0.0.0/0 10.10.10.13/32</b> . To add selectors, look at available ones via <b>pfctl -s state</b> .
<b>pfctl -z</b>	Clear all per rule statistics/counters

Command	Description
<b>pass in quick on egress from 62.13.77.141 to any</b>	<p>'Quick' rule, means allow this traffic to pass through on all interfaces, otherwise we would need 2nd rule allowing this traffic in <i>outgoing</i> direction on egress interface, to allow destined to ANY port/protocol with the source being <b>62.13.77.141</b> and destination being ANY IP address behind the PF firewall. NOTE: here, <b>egress</b> is not a direction, but a group name to which the interface in question (<b>em0</b>) belongs to. In OpenBSD you set it in a file <b>/etc/hostname.em0: group egress</b> or in real-time with the command: <b>ifconfig em0 group egress</b>.</p>