

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

Command	Description
pass in quick on egress from 62.13.77.141 to any	'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 62.13.77.141 and destination being ANY IP address behind the PF firewall. NOTE: here, egress is not a direction, but a group name to which the interface in question (em0) belongs to. In OpenBSD you set it in a file /etc/hostname.em0: group egress or in real-time with the command: ifconfig em0 group egress .