Linux and PF firewalls commands cheat sheet

Table of Contents

Firewalld daemon management (Red Hat based distributions)

Enable, disable, reload the daemon

Command	Description
systemctl disable/enable firewalld	Disable/enable firewalld, survives reboot.
systemctl stop firewalld	Stop firewalld until started manually or reboot.
firewall-cmd --reload	Reload firewall rules to make your changes active, keeping the state table. Active sessions do not disconnect. On finishing reload will output `success`.
systemctl restart firewalld	Restart the daemon, without resetting the active connections. Use in case of problems with the daemon.
firewall-cmd --complete-reload	Reload firewall completely, disconnecting the active connections. When nothing else helps.

List rules, status, additional info

Command	Description
firewall-cmd --state	Show firewall daemon status
firewall-cmd --list-all	List currently active rules
firewall-cmd --get-default-zone	Show the default zone for interfaces.
firewall-cmd --get-zones	List all available zones

Command	Description
firewall-cmd --get-active-zones	Show active zones, including to which zone each interface belongs.
firewall-cmd --list-all-zones	List all zones with their rules and associated interfaces.
firewall-cmd --add-service <service name>	Add predefined service by name to the default zone, with action ACCEPT, e.g. `firewall-cmd -add -service ftp` .

Open, close ports

Command	Description
firewall-cmd --add-port=*port-number* /*protocol*	Open in incoming *port-number* of the *protocol*. E.g. open incoming to TCP port 5900 from any: `firewall-cmd --add-port=5900/tcp`
firewall-cmd --remove-port=*port-number* /*protocol*	Close the open *port-number*. E.g. close the open port 5900/tcp: `firewall-cmd --remove -port=5900/tcp`
firewall-cmd --runtime-to-permanent	Make the changed rules permanent to survive reboot.

Ubuntu Uncomplicated Firewall (ufw)

Table 1. ufw management commands

Command	Description
ufw status	Show whether the firewall is on and if on, list the active rules.
ufw enable	Enable firewall.
ufw disable	Disable firewall
ufw reload	Reload firewall and rules.
ufw allow <predefined service name>	Allow some service in any direction from/to any IP address using so called `simple` rule syntax. The service names are as per `/etc/services`. E.g. to allow ssh from any: `ufw allow ssh`.
/etc/ufw/before.rules	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
pfct -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).
pass in quick on egress from 62.13.77.141 to any	'Quick' rule (means allows this traffic on all interfaces, otherwise we would need 2nd rule allowing this traffic in *outgoing* direction on egress interface) to allow incoming 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`.