Firewall-cmd Cheat Sheet

BY SETH KENLON

firewall-cmd is a command to adjust the settings of firewalld.

Start the firewall	
`systemctl enable --now firewalld`	enable and start the firewall

Global options	
`--permanent`	append to any command to make firewalld changes persistent
`--reload`	reload firewalld rules

Firewall-cmd: managing zones	
`--get-zones`	list all zones
`--get-active-zones`	list all active zones and all interfaces is each
`--zone=home --list-all`	list properties of zone `home`
`--change-interface=eth0 --zone=home`	add interface eth0 to zone `home`
`--get-default`	get default zone
`--set-default-zone home`	set default zone to `home`
`--new-zone=work`	create new zone `work` (requires rule reload)

Firewall-cmd: add ports and services	
`--get-services`	list all defined services
`--add-service murmur --zone=home`	allow traffic on `murmur` ports in zone `home`
`--add-port=123/tcp --zone=home`	allow TCP traffic on port 123 in zone `home`

Firewall-cmd: remove ports and services	
`--remove-port 123/tcp --zone=home`	deny traffic on port 123 in zone `home`
`--remove-service murmur --zone=home`	deny traffic on `murmur` ports in zone `home`

Direct rules	
Direct rules can be passed through firewall-cmd. This allows complex configuration, for instance, when you want to allow traffic to and from a virtual machine through a network bridge.	
`--direct --passthrough ipv6 -I FORWARD -o tap0 -j ACCEPT`	permit IPv6 traffic from tap0
`--direct --passthrough ipv6 -I FORWARD -i tap0 -j ACCEPT`	permit IPv6 traffic to tap0

