Cheatography

firewall-cmd Cheat Sheet

by Mikaël LE BERRE (mikael.leberre) via cheatography.com/113443/cs/21731/

Initial information	
Get the status of firewalld	firewall-cmd --state
Reload the firewall	firewall-cmd --reload
List of all supported zones	firewall-cmd --get-zones
List of all supported services	firewall-cmd --get-services
List of all supported icmptypes	firewall-cmd --get-icmptypes
List all zones with the enabled features	firewall-cmd --list-all-zones
Print zone with the enabled features	firewall-cmd [--zone=<zone>] --list-all
Get the default zone	firewall-cmd --get-default-zone
Set the default zone	firewall-cmd --set-default-zone=<zone>
Get active zones	firewall-cmd --get-active-zones
Get zone related to an interface	firewall-cmd --get-zone-of-interface=<interface>

Interface	
Add an interface to a zone	firewall-cmd [--zone=<zone>] --add-interface=<interface>
Change the zone an interface belongs to	firewall-cmd [--zone=<zone>] --change-interface=<interface>
Remove an interface from a zone	firewall-cmd [--zone=<zone>] --remove-interface=<interface>
Query if an interface is in a zone	firewall-cmd [--zone=<zone>] --query-interface=<interface>
List the enabled services in a zone	firewall-cmd [--zone=<zone>] --list-services

Service	
Enable a service in a zone	firewall-cmd [--zone=<zone>] --add-service=<service> [--timeout=<seconds>]
Disable a service in a zone	firewall-cmd [--zone=<zone>] --remove-service=<service>
Query if a service is enabled in a zone	firewall-cmd [--zone=<zone>] --query-service=<service>

Source	
Enable a source in a zone	firewall-cmd [--zone=<zone>] --add-source=<address> [--timeout=<seconds>]
Disable a source in a zone	firewall-cmd [--zone=<zone>] --remove-source=<address>
Query if a source is enabled in a zone	firewall-cmd [--zone=<zone>] --query-source=<address>

ICMP	
Enable ICMP blocks in a zone	firewall-cmd [--zone=<zone>] --add-icmp-block=<icmptype>
Disable ICMP blocks in a zone	firewall-cmd [--zone=<zone>] --remove-icmp-block=<icmptype>
Query ICMP blocks in a zone	firewall-cmd [--zone=<zone>] --query-icmp-block=<icmptype>
Example:	firewall-cmd --zone=public --add-icmp-block=echo-reply

By **Mikaël LE BERRE** (mikael.leberre)
cheatography.com/mikael-leberre/

Published 4th February, 2020.
Last updated 25th February, 2020.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Cheatography

firewall-cmd Cheat Sheet

by Mikaël LE BERRE (mikael.leberre) via cheatography.com/113443/cs/21731/

port and protocol combination

Enable a port and protocol combination in a zone	firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol> [--timeout=<-seconds>]
Disable a port and protocol combination in a zone	firewall-cmd [--zone=<zone>] --remove-port=<port>[-<port>]/<protocol>
Query if a port and protocol combination in enabled in a zone	firewall-cmd [--zone=<zone>] --query-port=<port>[-<port>]/<protocol>

port forwarding or port mapping

Enable port forwarding or port mapping in a zone	firewall-cmd [--zone=<zone>] --add-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
Disable port forwarding or port mapping in a zone	firewall-cmd [--zone=<zone>] --remove-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
Query port forwarding or port mapping in a zone	firewall-cmd [--zone=<zone>] --query-forward-port=port=<port>[-<port>]:proto=<protocol> { :toport=<port>[-<port>] | :toaddr=<address> | :toport=<port>[-<port>]:toaddr=<address> }
Example:	firewall-cmd --zone=home --add-forward-port=port=22:proto=tcp:toaddr=127.0.0.2

Permanent

The permanent options are not affecting runtime directly. These options are only available after a reload or restart. To have runtime and permanent setting, you need to supply both. The **–permanent** option needs to be the first option for all permanent calls.

panic mode

Enable panic	firewall-cmd --enable-panic
Disable panic mode	firewall-cmd --disable-panic
Query panic mode	firewall-cmd --query-panic

Block all network traffic in case of emergency

Masquerading

Enable masquerading in a zone	firewall-cmd [--zone=<zone>] --add-masquerade
Disable masquerading in a zone	firewall-cmd [--zone=<zone>] --remove-masquerade
Query masquerading in a zone	firewall-cmd [--zone=<zone>] --query-masquerade

By **Mikaël LE BERRE** (mikael.leberre)
cheatography.com/mikael-leberre/

Published 4th February, 2020.
Last updated 25th February, 2020.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Cheatography

firewall-cmd Cheat Sheet

by Mikaël LE BERRE (mikael.leberre) via cheatography.com/113443/cs/21731/

Direct options	
Pass a command through to the firewall. <args> can be all iptables, ip6tables and ebtables command line arguments	firewall-cmd --direct --passthrough { ipv4 | ipv6 | eb } <args>
Add a new chain <chain> to a table <table>.	firewall-cmd [--permanent] --direct --add-chain { ipv4 | ipv6 | eb } <table> <chain>
Remove a chain with name <chain> from table <table>.	firewall-cmd [--permanent] --direct --remove-chain { ipv4 | ipv6 | eb } <table> <chain>
Query if a chain with name <chain> exists in table <table>. Returns 0 if true, 1 otherwise.	firewall-cmd [--permanent] --direct --query-chain { ipv4 | ipv6 | eb } <table> <chain>
Get all chains added to table <table> as a space separated list.	firewall-cmd [--permanent] --direct --get-chains { ipv4 | ipv6 | eb } <table>
Add a rule with the arguments <args> to chain <chain> in table <table> with priority <priority>.	firewall-cmd [--permanent] --direct --add-rule { ipv4 | ipv6 | eb } <table> <chain> <priority> <args>
Remove a rule with the arguments <args> from chain <chain> in table <table>.	firewall-cmd [--permanent] --direct --remove-rule { ipv4 | ipv6 | eb } <table> <chain> <args>
Query if a rule with the arguments <args> exists in chain <chain> in table <table>. Returns 0 if true, 1 otherwise.	firewall-cmd [--permanent] --direct --query-rule { ipv4 | ipv6 | eb } <table> <chain> <args>
Get all rules added to chain <chain> in table <table> as a newline separated list of arguments.	firewall-cmd [--permanent] --direct --get-rules { ipv4 | ipv6 | eb } <table> <chain>

The direct options give a more direct access to the firewall. These options require user to know basic iptables concepts.

By **Mikaël LE BERRE** (mikael.leberre)
cheatography.com/mikael-leberre/

Published 4th February, 2020.
Last updated 25th February, 2020.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com