

Initial information

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

Interface

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

Service

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

Source

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

ICMP

Enable ICMP blocks in a zone	<code>firewall-cmd [--zone=<zone>] --add-icmp-block=<icmptype></code>
Disable ICMP blocks in a zone	<code>firewall-cmd [--zone=<zone>] --remove-icmp-block=<icmptype></code>
Query ICMP blocks in a zone	<code>firewall-cmd [--zone=<zone>] --query-icmp-block=<icmptype></code>

Example: `firewall-cmd --zone=public --add-icmp-block=echo-reply`



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

Published 4th February, 2020.
Last updated 25th February, 2020.
Page 1 of 3.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

port and protocol combination

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

port forwarding or port mapping

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

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	<code>firewall-cmd --enable-panic</code>
Disable panic mode	<code>firewall-cmd --disable-panic</code>
Query panic mode	<code>firewall-cmd --query-panic</code>
Block all network traffic in case of emergency	

Masquerading

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



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

Published 4th February, 2020.
Last updated 25th February, 2020.
Page 2 of 3.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

Direct options

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

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



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

Published 4th February, 2020.
Last updated 25th February, 2020.
Page 3 of 3.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>