Firewall-cmd: Direct Options

Direct options rules offer more complex options, using raw iptables syntax. These configuration rules provide more direct access to the firewall but require some basic iptables knowledge (as it has a similar syntax.)

The direct options are mainly reserved for use by services or applications to add specific firewalls. However, as discussed, they can also be used to add your own custom firewall rules.

Direct options use concepts such as tables, chains, commands, parameters, and targets, similar to the iptables command. In general, the first argument must be ipv4 or ipv6.

Direct options are configured within a file using an XML format and are mainly reserved for use by services or applications to add specific firewalls. However, they can also be used to add your own custom firewall rules. The following tags are required to create direct rules:

Tag	Description
<direct>	This start and end tag is required. It can only be used once in a direct config file.
<chain>	Option tag. Used to define named for custom chains. Has three attributes: ipv, table, and chain
<rule>	Optional element tag. Used to add rules to built-in or custom chains. Has four attributes: ipv, table, chain, or priority.

A firewalld direct configuration file contains information about permanent direct chains, rules and passthroughs. The example below presents the structure of a direct configuration file:

Direct Configuration File Structure

```
<?xml version="1.0" encoding="utf-8"?>
          <direct>
            [ <chain ipv="ipv4|ipv6|eb" table="table" chain="chain"/> ]
             [ <rule ipv="ipv4|ipv6|eb" table="table" chain="chain" priority="priority"> args
             </rule> ]
            [ <passthrough ipv="ipv4|ipv6|eb"> args </passthrough> ]
          </direct>
```

Note: It is advised to only use direct options if normal and rich-rules cannot be used.

Examples of Direct Rule Management: firewall-cmd

Below is an example of blacklisting the networks 192.168.1.0/24 and 192.168.5.0/24 with logging and dropping early in the raw table:

```
<?xml version="1.0" encoding="utf-8"?>
      <direct>
            <chain ipv="ipv4" table="raw" chain="blacklist"/>

            <rule ipv="ipv4" table="raw" chain="PREROUTING"
            priority="0">-s 192.168.1.0/24 -j blacklist</rule>

            <rule ipv="ipv4" table="raw" chain="PREROUTING"
            priority="1">-s 192.168.5.0/24 -j blacklist</rule>

            <rule ipv="ipv4" table="raw" chain="blacklist"
            priority="0">-m limit --limit 1/min -j LOG --log-prefix
            "blacklisted: "</rule>

            <rule ipv="ipv4" table="raw" chain="blacklist"
            priority="1">-j DROP</rule>

      </direct>
```

The capability to configure direct rules via `firewall-cmd` is also possible. (The fields in the above example still apply but the syntax is different and the actual tags are not required.)

Table Parameters

The table parameter is any one of the iptables' tables. Looking at the individual parameters, the chain indicates the particular chain you wish to add the rule to within the table you selected. The priority designates the rule order. (So a priority of 0 adds the rule to the top of the chain while a higher priority adds the rule further down in the chain.) The args parameter can be any valid option useable with the iptables command.

```
[--permanent] --direct --add-rule ipv4 <table> <chain> <priority> <args> …
```

Man page

To learn more about the firewalld direction options, please review the `firewalld.direct(5)` man page.