# Firewall-cmd: Rich Rules

If the basic syntax for `firewall-cmd` won’t address your needs, then you can add rich-rules. This syntax is more expressive than the `firewall-cmd` syntax and can handle complex rules. The rich-language uses keywords and values and is an abstract representation of iptables rules. It extends the normal rules with the ability to use additional source and destination addresses and logging.

Like iptables, a rule is part of a zone, and a zone contains several rules. The first rule in a zone that matches a packet “wins” and an action is taken based on that rule. Therefore, the rules that follow it will not be evaluated once a match has occurred.

The firewalld rich-rule is provided as a single line string within the `firewall-cmd` command. The general rule structure for rich-language is illustrated below:

**General Rich-Language Rule Structure**

```
rule [family=”ipv4|ipv6”]
      [source] [not] address=”address[/mask]”|mac=”mac-address”
      [destination] [not] address=”address[/mask]”
      service name=”service name” |
            port port=”port value” protocol=”tcp|udp” |
            protocol value=”protocol” |
            icmp-block name=”icmptype name” |
            masquerade |
            forward-port port=”port value” protocol=”tcp|udp” to-port=”port value” to-
      addr=”address” |
            source-port port=”port value” protocol=”tcp|udp”
      [log] [prefix=”prefix text”] [level=”log level”] [limit value=”rate/duration”]
      [audit] [limit value=”rate/duration”]
      [     accept [limit value=”rate/duration”] |
            reject [type=”reject type”] [limit value=”rate/duration”] |
            drop [limit value=”rate/duration”] |
            mark set=”mark[/mask]” [limit value=”rate/duration”]
      ]
```

**Note:** Not all parts of the rich-rule are necessary.

To view a list of the current rich-rules or to add a rich-rule using the format in the example above, use one of the following `firewall-cmd` options.

| Option | Description |
|---|---|
| `--list-rich-rules` | List the current rich rules |
| `--add-rich-rule='rule'` | Add a new rich-rule |

**Note:** When rich rules are added, they are added to the end of a chain. So, for example, if there was already an "allow all traffic" rule for SSH and you added a rule to block a specific host from connecting via SSH through rich rules, it would not work. The "allow all" rule would be matched first and the rest of the rules would not be evaluated in the chain.

Below are some examples of implementing Rich-Rule Management for `firewall-cmd`:

| Option | Description |
|---|---|
| `firewall-cmd --add-rich-rule='rule protocol value="ah" accept'` | Enable IPv4 connections for the ah protocol |
| `firewall-cmd --add-rich-rule='rule service name="ftp" log audit accept'` | Allow IPv4 ftp connection and log them using audit |
| `firewall-cmd -add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" service name="tftp" log prefix="tftp" level="info" limit value="1/m" accept'` | Allow connection from 192.168.0.0/24 for the tftp service and log 1 per minute using syslog |

## Man page

To learn more about the firewalld rich rules, please review the `firewalld.richlanguage(5)` man page.