



Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'firewalld.1'

\$ man firewalld.1

FIREWALLD(1) firewalld FIREWALLD(1)

NAME

firewalld - Dynamic Firewall Manager

SYNOPSIS

firewalld [OPTIONS...]

DESCRIPTION

firewalld provides a dynamically managed firewall with support for network/firewall zones to define the trust level of network connections or interfaces. It has support for IPv4, IPv6 firewall settings and for ethernet bridges and has a separation of runtime and permanent configuration options. It also supports an interface for services or applications to add firewall rules directly.

OPTIONS

These are the command line options of firewalld:

-h, --help

Prints a short help text and exits.

--default-config

Path to firewalld default configuration. This usually defaults to

/usr/lib/firewalld.

`--debug[=level]`

Set the debug level for firewalld to level. The range of the debug level is 1 (lowest level) to 10 (highest level). The debug output will be written to the firewalld log file specified by `--log-file`.

`--debug-gc`

Print garbage collector leak information. The collector runs every 10 seconds and if there are leaks, it prints information about the leaks.

`--log-target`

Define the output target to which log messages are written. In mixed mode, Firewalld writes info-level log messages to syslog. Debug messages are written to a file (see the `--log-file` parameter). Info messages also go to stdout and stderr. The syslog, file or console modes write all messages to the one configured target only.

`--log-file`

Define the file where debug messages are written to. The default file is `/var/log/firewalld`.

`--nofork`

Turn off daemon forking. Force firewalld to run as a foreground process instead of as a daemon in the background.

`--nopic`

Disable writing pid file. By default the program will write a pid file. If the program is invoked with this option it will not check for an existing server process.

`--system-config`

Path to firewalld system (user) configuration. This usually defaults to `/etc/firewalld`.

CONCEPTS

firewalld has a D-Bus interface for firewall configuration of services and applications. It also has a command line client for the user.

Services or applications already using D-Bus can request changes to the

firewall with the D-Bus interface directly. For more information on the firewalld D-Bus interface, please have a look at [firewalld.dbus\(5\)](#).

firewalld provides support for zones, predefined services and ICMP types and has a separation of runtime and permanent configuration options. Permanent configuration is loaded from XML files in `/usr/lib/firewalld` (`--default-config`) or `/etc/firewalld` (`--system-config`) (see the section called `?DIRECTORIES?`).

If NetworkManager is not in use and firewalld gets started after the network is already up, the connections and manually created interfaces are not bound to the zone specified in the `ifcfg` file. The interfaces will automatically be handled by the default zone. firewalld will also not get notified about network device renames. All this also applies to interfaces that are not controlled by NetworkManager if `NM_CONTROLLED=no` is set.

You can add these interfaces to a zone with `firewall-cmd` [`--permanent`] `--zone=zone --add-interface=interface`. If there is a `/etc/sysconfig/network-scripts/ifcfg-interface` file, firewalld tries to change the `ZONE=zone` setting in this file.

If firewalld gets reloaded, it will restore the interface bindings that were in place before reloading to keep interface bindings stable in the case of NetworkManager uncontrolled interfaces. This mechanism is not possible in the case of a firewalld service restart.

It is essential to keep the `ZONE=` setting in the `ifcfg` file consistent to the binding in firewalld in the case of NetworkManager uncontrolled interfaces.

Zones

A network or firewall zone defines the trust level of the interface used for a connection. There are several pre-defined zones provided by firewalld. Zone configuration options and generic information about zones are described in [firewalld.zone\(5\)](#)

Services

A service can be a list of local ports, protocols and destinations and additionally also a list of firewall helper modules automatically

loaded if a service is enabled. Service configuration options and generic information about services are described in `firewalld.service(5)`. The use of predefined services makes it easier for the user to enable and disable access to a service.

ICMP types

The Internet Control Message Protocol (ICMP) is used to exchange information and also error messages in the Internet Protocol (IP). ICMP types can be used in `firewalld` to limit the exchange of these messages.

For more information, please have a look at `firewalld.icmptype(5)`.

Runtime configuration

Runtime configuration is the actual active configuration and is not permanent. After reload/restart of the service or a system reboot, runtime settings will be gone if they haven't been also in permanent configuration.

Permanent configuration

The permanent configuration is stored in config files and will be loaded and become new runtime configuration with every machine boot or service reload/restart.

Direct interface

DEPRECATED

The direct interface has been deprecated. It will be removed in a future release. It is superseded by policies, see `firewalld.policies(5)`.

The direct interface is mainly used by services or applications to add specific firewall rules. It requires basic knowledge of `ip(6)` tables concepts (tables, chains, commands, parameters, targets).

DIRECTORIES

`firewalld` supports two configuration directories:

Default/Fallback configuration in `/usr/lib/firewalld` (`--default-config`)

This directory contains the default and fallback configuration provided by `firewalld` for `icmptypes`, services and zones. The files provided with the `firewalld` package should not get changed and the changes are gone with an update of the `firewalld` package. Additional `icmptypes`, services

and zones can be provided with packages or by creating files.

System configuration settings in `/etc/firewalld` (`--system-config`)

The system or user configuration stored here is either created by the system administrator or by customization with the configuration interface of `firewalld` or by hand. The files will overload the default configuration files.

To manually change settings of pre-defined `icmptypes`, zones or services, copy the file from the default configuration directory to the corresponding directory in the system configuration directory and change it accordingly.

For more information on `icmptypes`, please have a look at the `firewalld.icmptype(5)` man page, for services at `firewalld.service(5)` and for zones at `firewalld.zone(5)`.

SIGNALS

Currently only `SIGHUP` is supported.

SIGHUP

Reloads the complete firewall configuration. You can also use `firewall-cmd --reload`. All runtime configuration settings will be restored. Permanent configuration will change according to options defined in the configuration files.

SEE ALSO

`firewall-applet(1)`, `firewalld(1)`, `firewall-cmd(1)`, `firewall-config(1)`,
`firewalld.conf(5)`, `firewalld.direct(5)`, `firewalld.dbus(5)`,
`firewalld.icmptype(5)`, `firewalld.lockdown-whitelist(5)`, `firewall-offline-cmd(1)`, `firewalld.richlanguage(5)`, `firewalld.service(5)`,
`firewalld.zone(5)`, `firewalld.zones(5)`, `firewalld.policy(5)`,
`firewalld.policies(5)`, `firewalld.ipset(5)`, `firewalld.helper(5)`

NOTES

`firewalld` home page:

<http://firewalld.org>

More documentation with examples:

<http://fedoraproject.org/wiki/FirewallD>

AUTHORS

Thomas Woerner <twoerner@redhat.com>

Developer

Jiri Popelka <jpopelka@redhat.com>

Developer

Eric Garver <eric@garver.life>

Developer

firewalld 1.2.1

FIREWALLD(1)