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

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'firewalld.conf.5' command

$ man firewalld.conf.5

FIREWALLD.CONF(5) firewalld.conf FIREWALLD.CONF(5)

NAME

firewalld.conf - firewalld configuration file

SYNOPSIS

/etc/firewalld/firewalld.conf

DESCRIPTION

firewalld.conf is loaded by firewalld during the initialization process. The file contains the basic configuration options for firewalld.

OPTIONS

These are the options that can be set in the config file:

DefaultZone

This sets the default zone for connections or interfaces if the zone is not selected or specified by NetworkManager, initscripts or command line tool. The default zone is public.

MinimalMark

Deprecated. This option is ignored and no longer used. Marks are no longer used internally.

CleanupModulesOnExit

Setting this option to yes or true unloads all firewall-related kernel modules when firewalld is stopped. The default value is no or false.

CleanupOnExit

If firewalld stops, it cleans up all firewall rules. Setting this option to no or false leaves the current firewall rules untouched. The default value is yes or true.

Lockdown

If this option is enabled, firewall changes with the D-Bus interface will be limited to applications that are listed in the lockdown whitelist (see firewalld.lockdown-whitelist(5)). The default value is no or false.

IPv6_rpfilter

If this option is enabled (it is by default), reverse path filter test on a packet for IPv6 is performed. If a reply to the packet would be sent via the same interface that the packet arrived on, the packet will match and be accepted, otherwise dropped. For IPv4 the rp_filter is controlled using sysctl.

Note: This feature has a performance impact. In most cases the impact is not enough to cause a noticeable difference. It requires route lookups and its execution occurs before the established connections fast path. As such it can have a significant performance impact if there is a lot of traffic. It's enabled by default for security, but can be disabled if performance is a concern.

IndividualCalls

If this option is disabled (it is by default), combined -restore calls are used and not individual calls to apply changes to the firewall. The use of individual calls increases the time that is needed to apply changes and to start the daemon, but is good for debugging as error messages are more specific.

LogDenied

Add logging rules right before reject and drop rules in the INPUT, FORWARD and OUTPUT chains for the default rules and also final reject and drop rules in zones for the configured link-layer packet type. The possible values are: all, unicast, broadcast, multicast and off. The default setting is off, which disables the logging.

AutomaticHelpers

Deprecated. This option is ignored and no longer used.

FirewallBackend

Selects the firewall backend implementation. Possible values are; nftables (default), or iptables. This applies to all firewalld primitives. The only exception is direct and passthrough rules which always use the traditional iptables, ip6tables, and ebtables backends.

Note: The iptables backend is deprecated. It will be removed in a future release.

FlushAllOnReload

Flush all runtime rules on a reload. In previous releases some runtime configuration was retained during a reload, namely; interface to zone assignment, and direct rules. This was confusing to users. To get the old behavior set this to "no". Defaults to "yes".

RFC3964_IPv4

As per RFC 3964, filter IPv6 traffic with 6to4 destination addresses that correspond to IPv4 addresses that should not be routed over the public internet. Defaults to "yes".

AllowZoneDrifting

Deprecated. This option is ignored and no longer used.

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