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.zones.5'

$ man firewalld.zones.5

FIREWALLD.ZONES(5) firewalld.zones FIREWALLD.ZONES(5)

NAME

firewalld.zones - firewalld zones

DESCRIPTION

What is a zone?

A network zone defines the level of trust for network connections. This is a one to many relation, which means that a connection can only be part of one zone, but a zone can be used for many network connections.

The zone defines the firewall features that are enabled in this zone:

Intra Zone Forwarding

Allows packets received by a zone to be forwarded to other interfaces or sources within the same zone, even if the zone's target is not ACCEPT.

Predefined services

A service is a combination of port and/or protocol entries. Optionally netfilter helper modules can be added and also a IPv4 and IPv6 destination address.

Ports and protocols

Definition of tcp, udp, sctp or dccp ports, where ports can be a single port or a port range.

ICMP blocks

Blocks selected Internet Control Message Protocol (ICMP) messages. These messages are either information requests or created as a reply to information requests or in error conditions.

ICMP block inversion

Changes how ICMP messages are handled. When enabled, all ICMP message types are blocked, except for those in the ICMP block list.

Masquerading

The addresses of a private network are mapped to and hidden behind a public IP address. This is a form of address translation.

Forward ports

A forward port is either mapped to the same port on another host or to another port on the same host or to another port on another host.

Rich language rules

The rich language extends the elements (service, port, icmp-block, masquerade, forward-port and source-port) with additional source and destination addresses, logging, actions and limits for logs and actions. It can also be used for host or network white and black listing (for more information, please have a look at firewalld.richlanguage(5)).

For more information on the zone file format, please have a look at firewalld.zone(5).

Which zones are available?

Here are the zones provided by firewalld sorted according to the default trust level of the zones from untrusted to trusted:

drop

Any incoming network packets are dropped, there is no reply. Only outgoing network connections are possible.

block

Any incoming network connections are rejected with an icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6. Only network connections initiated within this system are possible.

public

For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.

external

For use on external networks with masquerading enabled especially for routers. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.

dmz

For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted.

work

For use in work areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.

home

For use in home areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.

internal

For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.

trusted

All network connections are accepted.

Which zone should be used?

A public WIFI network connection for example should be mainly untrusted, a wired home network connection should be fairly trusted.

Select the zone that best matches the network you are using.

How to configure or add zones?

To configure or add zones you can either use one of the firewalld interfaces to handle and change the configuration: These are the graphical configuration tool firewall-config, the command line tool firewall-cmd or the D-Bus interface. Or you can create or copy a zone file in one of the configuration directories. /usr/lib/firewalld/zones is used for default and fallback configurations and /etc/firewalld/zones is used for user created and customized configuration files.

How to set or change a zone for a connection?

The zone is stored into the ifcfg of the connection with ZONE= option. If the option is missing or empty, the default zone set in firewalld is used.

If the connection is controlled by NetworkManager, you can also use nm-connection-editor to change the zone.

For the addition or change of interfaces that are not under control of NetworkManager: firewalld tries to change the ZONE setting in the ifcfg file, if an ifcfg file exists that is using the interface.

Only for the removal of interfaces that are not under control of NetworkManager: firewalld is not trying to change the ZONE setting in the ifcfg file. This is needed to make sure that an ifdown of the interface will not result in a reset of the zone setting to the default zone. Only the zone binding is then removed in firewalld then.

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