



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.zone.5'

\$ man firewalld.zone.5

FIREWALLD.ZONE(5) firewalld.zone FIREWALLD.ZONE(5)

NAME

firewalld.zone - firewalld zone configuration files

SYNOPSIS

/etc/firewalld/zones/zone.xml

/usr/lib/firewalld/zones/zone.xml

DESCRIPTION

A firewalld zone configuration file contains the information for a zone. These are the zone description, services, ports, protocols, icmp-blocks, masquerade, forward-ports, intra-zone forwarding and rich language rules in an XML file format. The file name has to be zone_name.xml where length of zone_name is currently limited to 17 chars.

This is the structure of a zone configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<zone [version="versionstring"] [target="ACCEPT|%%REJECT%%|DROP"]>
  [ <interface name="string"/> ]
  [ <source address="address[/mask]"|mac="MAC"|ipset="ipset"/> ]
```

```

[ <icmp-block-inversion/> ]
[ <forward/> ]
[ <short>short description</short> ]
[ <description>description</description> ]
[ <service name="string"/> ]
[ <port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> ]
[ <protocol value="protocol"/> ]
[ <icmp-block name="string"/> ]
[ <masquerade/> ]
[ <forward-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp" [to-port="portid[-portid]" [to-addr="IP address"]/>
]
[ <source-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> ]
[
  <rule [family="ipv4|ipv6"] [priority="priority"]>
    [ <source address="address[/mask]"|mac="MAC"|ipset="ipset" [invert="True"]/> ]
    [ <destination address="address[/mask]"|ipset="ipset" [invert="True"]/> ]
    [
      <service name="string"/> |
      <port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> |
      <protocol value="protocol"/> |
      <icmp-block name="icmptype"/> |
      <icmp-type name="icmptype"/> |
      <masquerade/> |
      <forward-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp" [to-port="portid[-portid]"
[to-addr="address"]/>
    ]
    [
      <log [prefix="prefix text"] [level="emerg|alert|crit|err|warn|notice|info|debug"]> [<limit
value="rate/duration"/>] </log> |
      <nflog [group="group id"] [prefix="prefix text"] [queue-size="threshold"]> [<limit value="rate/duration"/>]
</nflog>
    ]
  ]
  [ <audit> [<limit value="rate/duration"/>] </audit> ]

```

```

    [
      <accept> [<limit value="rate/duration"/>] </accept> |
      <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
      <drop> [<limit value="rate/duration"/>] </drop> |
      <mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>
    ]
  </rule>
]
</zone>

```

The config can contain these tags and attributes. Some of them are mandatory, others optional.

zone

The mandatory zone start and end tag defines the zone. This tag can only be used once in a zone configuration file. There are optional attributes for zones:

version="string"

To give the zone a version.

target="ACCEPT|%%REJECT%%|DROP"

Can be used to accept, reject or drop every packet that doesn't match any rule (port, service, etc.). The ACCEPT target is used in trusted zone to accept every packet not matching any rule. The %%REJECT%% target is used in block zone to reject (with default firewalld reject type) every packet not matching any rule. The DROP target is used in drop zone to drop every packet not matching any rule. If the target is not specified, every packet not matching any rule will be rejected.

interface

Is an optional empty-element tag and can be used several times. It can be used to bind an interface to a zone. You don't need this for NetworkManager-managed interfaces, because NetworkManager binds interfaces to zones automatically. See also 'How to set or change a zone for a connection?' in firewalld.zones(5). You can use it as a fallback mechanism for interfaces that can't be managed via

NetworkManager. An interface entry has exactly one attribute:

name="string"

The name of the interface to be bound to the zone.

source

Is an optional empty-element tag and can be used several times. It can be used to bind a source address, address range, a MAC address or an ipset to a zone. A source entry has exactly one of these attributes:

address="address[/mask]"

The source is either an IP address or a network IP address with a mask for IPv4 or IPv6. The network family (IPv4/IPv6) will be automatically discovered. For IPv4, the mask can be a network mask or a plain number. For IPv6 the mask is a plain number. The use of host names is not supported.

mac="MAC"

The source is a MAC address. It must be of the form

XX:XX:XX:XX:XX:XX.

ipset="ipset"

The source is an ipset.

icmp-block-inversion

Is an optional empty-element tag and can be used only once in a zone configuration. This flag inverts the icmp block handling. Only enabled ICMP types are accepted and all others are rejected in the zone.

forward

Is an optional empty-element tag and can be used only once in a zone configuration. This flag enables intra-zone forwarding. When enabled, packets will be forwarded between interfaces or sources within a zone, even if the zone's target is not set to ACCEPT.

short

Is an optional start and end tag and is used to give a more readable name.

description

Is an optional start and end tag to have a description.

service

Is an optional empty-element tag and can be used several times to have more than one service entry enabled. A service entry has exactly one attribute:

name="string"

The name of the service to be enabled. To get a list of valid service names `firewall-cmd --get-services` can be used.

port

Is an optional empty-element tag and can be used several times to have more than one port entry. All attributes of a port entry are mandatory:

port="portid[-portid]"

The port can either be a single port number `portid` or a port range `portid-portid`.

protocol="tcp|udp|sctp|dccp"

The protocol can either be `tcp`, `udp`, `sctp` or `dccp`.

protocol

Is an optional empty-element tag and can be used several times to have more than one protocol entry. All protocol has exactly one attribute:

value="string"

The protocol can be any protocol supported by the system. Please have a look at `/etc/protocols` for supported protocols.

icmp-block

Is an optional empty-element tag and can be used several times to have more than one `icmp-block` entry. Each `icmp-block` tag has exactly one mandatory attribute:

name="string"

The name of the Internet Control Message Protocol (ICMP) type to be blocked. To get a list of valid ICMP types `firewall-cmd --get-icmptypes` can be used.

tcp-mss-clamp

Is an optional empty-element tag and can be used several times. If left empty maximum segment size is set to 'pmtu'. This tag has exactly one optional attribute:

value="string"

Value can set maximum segment size to 'pmtu' (Path Maximum Transmission Unit) or a user-defined value that is greater than or equal to 536.

masquerade

Is an optional empty-element tag. It can be used only once. If it's present masquerading is enabled.

forward-port

Is an optional empty-element tag and can be used several times to have more than one port or packet forward entry. There are mandatory and also optional attributes for forward ports:

Mandatory attributes:

The local port and protocol to be forwarded.

`port="portid[-portid]"`

The port can either be a single port number portid or a port range portid-portid.

`protocol="tcp|udp|sctp|dccp"`

The protocol can either be tcp, udp, sctp or dccp.

Optional attributes:

The destination of the forward. For local forwarding add to-port only. For remote forwarding add to-addr and use to-port optionally if the destination port on the destination machine should be different.

`to-port="portid[-portid]"`

The destination port or port range to forward to. If omitted, the value of the port= attribute will be used altogether with the to-addr attribute.

`to-addr="address"`

The destination IP address either for IPv4 or IPv6.

source-port

Is an optional empty-element tag and can be used several times to have more than one source port entry. All attributes of a source port entry are mandatory:

`port="portid[-portid]"`

The port can either be a single port number portid or a port range portid-portid.

protocol="tcp|udp|sctp|dccp"

The protocol can either be tcp, udp, sctp or dccp.

rule

Is an optional element tag and can be used several times to have more than one rich language rule entry.

The general rule structure:

```
<rule [family="ipv4|ipv6"] [priority="priority"]>
  [ <source address="address[/mask]"|mac="MAC"|ipset="ipset" [invert="True"]/> ]
  [ <destination address="address[/mask]"|ipset="ipset" [invert="True"]/> ]
  [
    <service name="string"/> |
    <port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> |
    <protocol value="protocol"/> |
    <icmp-block name="icmptype"/> |
    <icmp-type name="icmptype"/> |
    <masquerade/> |
    <forward-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp" [to-port="portid[-portid]] [to-addr="address"]/> |
    <source-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> |
  ]
  [
    <log [prefix="prefix text"] [level="emerg|alert|crit|err|warn|notice|info|debug"]> [<limit value="rate/duration"/>]
  ]
</log> |
  <nflog [group="group id"] [prefix="prefix text"] [queue-size="threshold"]> [<limit value="rate/duration"/>] </nflog>
]
[ <audit> [<limit value="rate/duration"/>] </audit> ]
[
  <accept> [<limit value="rate/duration"/>] </accept> |
  <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
  <drop> [<limit value="rate/duration"/>] </drop> |
  <mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>
]
```

```
</rule>
```

Rule structure for source black or white listing:

```
<rule [family="ipv4|ipv6"] [priority="priority"]>
  <source address="address[/mask]"|mac="MAC"|ipset="ipset" [invert="True"]/>
  [
    <log [prefix="prefix text"] [level="emerg|alert|crit|err|warn|notice|info|debug"]> [<limit value="rate/duration"/>]
  </log> |
    <nflog [group="group id"] [prefix="prefix text"] [queue-size="threshold"]> [<limit value="rate/duration"/>] </nflog>
  ]
  [ <audit> [<limit value="rate/duration"/>] </audit> ]
  <accept> [<limit value="rate/duration"/>] </accept> |
  <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
  <drop> [<limit value="rate/duration"/>] </drop>
</rule>
```

For a full description on rich language rules, please have a look at `firewalld.richlanguage(5)`.

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 <jpapelka@redhat.com>

Developer

Eric Garver <eric@garver.life>

Developer

firewalld 1.2.1

FIREWALLD.ZONE(5)