Rocky Enterprise Linux 9.2 Manual Pages on command 'firewalld.policy.5'

$ man firewalld.policy.5

FIREWALLD.POLICY(5) firewalld.policy FIREWALLD.POLICY(5)

NAME

firewalld.policy - firewalld policy configuration files

SYNOPSIS

/etc/firewalld/policies/policy.xml

/usr/lib/firewalld/policies/policy.xml

DESCRIPTION

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

This is the structure of a policy configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<policy [version="versionstring"] [target="CONTINUE|ACCEPT|REJECT|DROP"] [priority="priority"]>
  [ <ingress-zone name="zone"/> ]
  [ <egress-zone name="zone"/> ]
  [ <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>
    ]
</policy>
```

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

policy

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

version="string"

To give the policy a version.

target="CONTINUE|ACCEPT|REJECT|DROP"

Can be used to accept, reject or drop every packet that doesn't match any rule (port, service, etc.). The CONTINUE is the default and used for policies that are non-terminal.

ingress-zone

An optional element that can be used several times. It can be the name of a firewalld zone or one of the symbolic zones: HOST, ANY. See firewalld.policies(5) for information about symbolic zones.

egress-zone

An optional element that can be used several times. It can be the name of a firewalld zone or one of the symbolic zones: HOST, ANY. See firewalld.policies(5) for information about symbolic zones.

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 <jpopelka@redhat.com>

Developer

Eric Garver <eric@garver.life>