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.policies.5'

$ man firewalld.policies.5

```
FIREWALLD.POLICIES(5)       firewalld.policies       FIREWALLD.POLICIES(5)

NAME
       firewalld.policies - firewalld policies

DESCRIPTION
   What is a policy?
       A policy applies a set of rules to traffic flowing between between
       zones (see zones (see firewalld.zones(5)). The policy affects traffic
       in a stateful unidirectional manner, e.g. zoneA to zoneB. This allows
       asynchronous filtering policies.

       A policy's relationship to zones is defined by assigning a set of
       ingress zones and a set of egress zones. For example, if the set of
       ingress zones contains "public" and the set of egress zones contains
       "internal" then the policy will affect all traffic flowing from the
       "public" zone to the "internal" zone. However, since policies are
       unidirectional it will not apply to traffic flowing from "internal" to
       "public". Note that the ingress set and egress set can contain multiple
       zones.

   Active Policies
```

Policies only become active if all of the following are true.

? The ingress zones list contain at least one regular zone or a single symbolic zone.

? The egress zones list contain at least one regular zone or a single symbolic zone.

? For non symbolic zones, the zone must be active. That is, it must have interfaces or sources assigned to it.

If the policy is not active then the policy has no effect.

Symbolic Zones

Regular zones are not enough to express every form of packet filtering. For example there is no zone to represent traffic flowing to or from the host running firewalld. As such, there are some symbolic zones to fill these gaps. However, symbolic zones are unique in that they're the only zone allowed in the ingress or egress zone sets. For example, you cannot use "public" and "HOST" in the ingress zones.

Symbolic zones:

1. HOST

   This symbolic zone is for traffic flowing to or from the host running firewalld. This corresponds to netfilter (iptables/nftables) chains INPUT and OUTPUT.

   ? If used in the egress zones list it will apply to traffic on the INPUT chain.

   ? If used in the ingress zones list it will apply to traffic on the OUTPUT chain.

2. ANY

   This symbolic zone behaves like a wildcard for the ingress and egress zones. With the exception that it does not include "HOST". It's useful if you want a policy to apply to every zone.

   ? If used in the ingress zones list it will apply for traffic originating from any zone.

   ? If used in the egress zones list it will apply for traffic destined to any zone.

Predefined Policies

firewalld ships with some predefined policies. These may or may not be active by default. For details see the description of each policy.

? allow-host-ipv6

Similarity to Zones

Policies are similar to zones in that they are an attachment point for firewalld's primitives: services, ports, forward ports, etc. This is not a coincidence. Policies are a generalization of how zones have traditionally achieved filtering. In fact, in modern firewalld zones are internally implemented as a set of policies.

The main difference between policies and zones is that policies allow filtering in all directions: input, output, and forwarding. With a couple of exceptions zones only allow input filtering which is sufficient for an end station firewalling. However, for network level filtering or filtering on behalf of virtual machines and containers something more flexible, i.e. policies, are needed.

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