Table Of Contents

CentOS / RHEL IPv6 ip6tables Firewall Configuration

Posted by Vivek Gite <vivek@nixcraft.com>

I know how to configure iptables (IPv4) host-based firewall using Netfilter. How do I configure ip6tables for basic filtering IPv6 packets?

[1]

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. The following configuration is tested on:

1. CentOS Linux 5.x
2. Red Hat Enterprise Linux 5.x
3. Fedora Linux 10 and 11.

[2]

Type the following command to see current ipv6 firewall configuration:

```
# ip6tables -nL --line-numbers
```

If no rules appear, activate IPv6 firewall and ensure that it starts at boot by typing the following command:

[3]

```
# chkconfig ip6tables on
```

/etc/sysconfig/ip6tables

Edit /etc/sysconfig/ip6tables, enter:

```
# vi /etc/sysconfig/ip6tables
```

You will see default rules as follows:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmpv6 -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d ff02::fb -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 32768:61000 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 32768:61000 ! --syn -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

To open port 80 (Http server) add the following before COMMIT line:

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT
```

To open port 53 (DNS Server) add the following before COMMIT line:

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m udp -p tcp --dport 53 -j ACCEPT
```

To open port 443 (Https server) add the following before COMMIT line:

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 443 -j ACCEPT
```

To open port 25 (smtp server) add the following before COMMIT line:

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 25 -j ACCEPT
```

To log before dropping all packets that are not explicitly accepted by previous rules, change the final lines from:

```
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

To:

```
-A RH-Firewall-1-INPUT -j LOG
-A RH-Firewall-1-INPUT -j DROP
COMMIT
```

Save and close the file. Restart ip6tables firewall:

```
# service ip6tables restart
# ip6tables -vnL --line-numbers
```

Sample Outputs:

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1    42237 3243K RH-Firewall-1-INPUT  all      *       *       ::/0                 ::/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 RH-Firewall-1-INPUT  all      *       *       ::/0                 ::/0

Chain OUTPUT (policy ACCEPT 12557 packets, 2042K bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain RH-Firewall-1-INPUT (2 references)
num   pkts bytes target     prot opt in     out     source               destination
1        6   656 ACCEPT     all      lo     *       ::/0                 ::/0
2    37519 2730K ACCEPT     icmpv6   *       *       ::/0                  ::/0
3        0     0 ACCEPT     esp      *       *       ::/0                 ::/0
4        0     0 ACCEPT     ah       *       *       ::/0                 ::/0
5      413 48385 ACCEPT     udp      *       *       ::/0                 ff02::fb/128
6        0     0 ACCEPT     udp      *       *       ::/0                 ::/0
7        0     0 ACCEPT     tcp      *       *       ::/0                 ::/0
8      173 79521 ACCEPT     udp      *       *       ::/0                 ::/0
9        0     0 ACCEPT     tcp      *       *       ::/0                 ::/0
10       0     0 ACCEPT     tcp      *       *       ::/0                 ::/0
11       0     0 ACCEPT     tcp      *       *       ::/0                 ::/0
12       0     0 ACCEPT     tcp      *       *       ::/0                 ::/0
13    4108  380K ACCEPT     udp      *       *       ::/0                 ::/0
14      18  4196 REJECT     all      *       *       ::/0                 ::/0
```

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/redhat-fedora-ip6tables-firewall-configuration/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/redhat-and-friends/**
[2] Image: **http://www.cyberciti.biz/faq/category/centos/**
[3] Image: **http://www.cyberciti.biz/faq/category/fedora-linux/**