Configuring iptables for IP multicast

klebers | *Nov 28 2012* | *Visits (50455)* 1

by: Kleber Sacilotto de Souza

Share

The default iptables rules that come with most of the Enterprise Linux distributions (e.g. RHEL and SLES) prevent multicast IP packets from reaching client applications that have joined multicast groups. This article will explain how to configure or disable iptables so client multicast applications can receive multicast packets.

Disabling iptables

If your multicast client system doesn't need to be protected by a firewall the easiest way to make a multicast application to work is by disabling iptables or any other firewall service that might be running. That can be done temporarily by flushing all the iptables rules with the following command:

```
# iptables -F
```

This command will disable all the iptables rules, however, the rules will be reloaded on the next system reboot.

The iptables rules can also be prevented from being loaded during the system boot. On RHEL systems it can be done by disabling the *iptables* service:

```
# chkconfig iptables off
```

On SLES system it can be done by disabling the firewall on Yast interface, or disabling the *SuSEfirewall2_init* and *SuSEfirewall2_setup* services:

```
# chkconfig SuSEfirewall2_init off
# chkconfig SuSEfirewall2_setup off
```

Configuring the iptables rules

If your multicast client system needs to have a firewall service running, the firewall will have to be configured to allow multicast packets. This section will show how to configure the iptables rules on a RHEL system.

The file */etc/sysconfig/iptables* is the configuration file that contains the iptables rules that will be loaded during the *iptables* service start. By adding the following line to this file, iptables will allow all incoming multicast packets:

```
 -A INPUT -m pkttype --pkt-type multicast -j ACCEPT
```

The order of the lines in the file is important, so the example rule above needs to be placed before the default rule that rejects all packets that don't fit in any of the previous rules. Following is an example of a complete configuration file:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j
ACCEPT
-A INPUT -m pkttype --pkt-type multicast -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

This example adds a rule to allow all incoming multicast packets. However, you might want to allow packets that arrive only to a specific network interface, from a certain range of source address or from a certain broadcast group. For more specific configurations, refer to the iptables man page.

Tags: *firewall network multicast*