Subject: error with multiple containers using libipq and iptables QUEUE targets
Posted by jeffa on Mon, 20 Jul 2009 23:38:44 GMT
View Forum Message <> Reply to Message

I have two running containers and in each I can insert an iptables rule such as:

iptables -t mangle -A PREROUTING -p icmp -j QUEUE

I have a sample program that uses libipq to fetch packets in userspace from the netfilter QUEUE target. Here is pseudo-code from that program:

```
raw_ip4_socket = socket(PF_INET, SOCK_RAW, IPPROTO_RAW);
h4 = ipq_create_handle(0, PF_INET);
err = ipq_set_mode(h4, IPQ_COPY_PACKET, BUFSIZE);
err = ipq_read(h4, buf, BUFSIZE, 0);
type = ipq_message_type(buf);
if (NLMSG_ERROR == type) {
   printf("received error message (%d): %s\n",
         ipq_get_msgerr(buf), ipq_errstr());
}
```

Now when I run this program on the first container, it works fine! I can get packets as expected into my userspace program, for example when I run ping.

However when I start the program on the second container, I receive netlink error messages from the kernel from ipq_read() (sample output is: "received error message (16): Unknown error"). Then I never receive any valid packets.

If I look at the iptables stats using "iptables -nvL -t mangle" the kernel says that the packets are hitting the QUEUE targets. Each machine shows correct packet counts. I am using 2.6.18-128.1.1.el5.028stab062.3. Any ideas?