Subject: Re: nat iptables SNAT problem
Posted by marcin4 on Sun, 02 Mar 2014 21:44:41 GMT
View Forum Message <> Reply to Message

It been always happening, even with older kernel.
I did more checking and tracing of the packages. this is what I discovered, but first let me describe the topography of my network.

block of public ips and number of servers on it.
openvz server has one of public ips,
some containers on openvz HN also have public ip addresses and
a bunch of containers in the same openvz HN have private ips netted by the same HN.
Since masquerade do not work with openvz I am using -j SNAT --to-source $WIP where $WIP is public IP address of HN.

The issue is, again not always, when the private IP containers try to access other servers on same block of public IPs.
the trace shows that these other servers see the packages coming from private IP address not from public IP of HN.
The accessing any other resource from outside my network works just fine and all the time.
CT with private IP send the UDP package to server A on public IP.
Server A sees the private IP as a source of the package.
The conclusion is that the iptables SNAT is not rewriting the source IP :

iptables -t nat -A POSTROUTING -s 10.0.1.0/24 -o $IF1 -j SNAT --to-source $WIP
where $IF1 is a eth device with public IP of HD and $WIP is the public IP of HN

If I stop the private IP CT for 30 sec or so and then restart it, everything works as it should for while (days)

I probably made this too complicated, but please try to follow my logic.
Thank you in advance