I've got a few vms i run using KVM. I want to make it so that the vms/guests can't use smtp or send any out any email to prevent abuse.

I've got some iptable rules in place on the host machine attempting to block the guest vms from making outgoing connections to ports 25 and 587, but they don't seem to be working

so i have ran this on the host machine:

iptables -I FORWARD -o br0 -p tcp --dport 25 -j DROP

iptables -I FORWARD -o br0 -p tcp --dport 587 -j DROP

then from one of the guests, i ran as a test telnet smtp.sendgrid.net 25 and it still connects/establishes a connection. Does anyone know what i'm doing wrong?

Here is my iptables ruleset: http://pastebin.com/raw/y5uDZEDa -- ive got the 2 iptables commands i just referenced at the top of the forward chain as well (from googling i read something about that).. but im still able to telnet smtp.sendgrid.net 25 or 587 on the guest vms

Running CentOS 7.2

EDIT: Looks like I figured it out. I just needed to run and enable this on the host machine: net.bridge.bridge-nf-call-iptables

sysctl net.bridge.bridge-nf-call-iptables=1

Now from the guest vms, i cant make outgoing connections to port 25 or 587, what i wanted, perfect

But I've been told with net.bridge.bridge-nf-call-iptables=1 all sorts of things can break, any bridged IP traffic will go through netfilter now

Given that my iptable ruleset is this only: http://pastebin.com/raw/gYJkub45 -- this rule set is most likely not going to change.. looking at that,
can you see anything being broken with bridged IP traffic going through netfilter ?