Subject: Iptables connlimit rule does nothing inside CT
Posted by dbassett on Mon, 17 Jun 2013 21:11:57 GMT
View Forum Message <> Reply to Message

I am running 2.6.32-042stab076.8 on a CentOS6 HN with CentOS6 containers, vzctl-4.2-1.x86_64. I have two containers running on the same HN. Each CT has a veth device. Both CT's veth device is connected to the same bridge device on the HN. They are assigned the addresses 192.168.0.1/24 and 192.168.0.2/24 and can ping each other.

On the HN I am able to modprobe the connlimit module (xt_connlimit). I can then use iptables rules on the hostnode such as:

iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 1 --connlimit-mask=32 -j REJECT

If I then attempt to initiate more than one ssh session to this HN from the same host, the second (and all subsequent) ssh connections are rejected.

I am able to successfully insert the same rule into the iptables configuration in either of my containers, which leads me to believe that the xt_connlimit module is properly loaded. However, I can create more than one successful ssh session, meaning that the iptables rule in the CT is not being matched for some reason. I have both "xt_limit" and "xt_connlimit" in the list of iptables modules to load in vz.conf. When I am running these tests, I have no iptables rules loaded on the HN, and I have no other iptables rules loaded in the container.

One interesting thing I have noticed is that when I enter a container on this hostnode, I get the following errors:

[root@hn0 ~]# vzctl enter 2033892
Warning: Unknown iptable module: xt_connlimit, skipped
Warning: Unknown iptable module: xt_limit, skipped

It seems like this might be related to my issue, but it might just be a red herring.

Am I missing something obvious here? Or is this a bug with OpenVZ?