Subject: Re: Is OpenVZ in Parallels vm known to work?
Posted by Vasily Tarasov on Mon, 14 May 2007 10:11:10 GMT
View Forum Message <> Reply to Message

Hello,

I've just tried to reproduce the problem:

HN: Centos 4.4
VE: Centos 4.4
vzctl: 3.0.16
kernel: 2.6.18-028stab031

I added ipt_state module to vz.conf file and loaded this module on HN, then I started VE and used system-config-securitylevel utility in VE to mark venet0 as trusted interface and allow ssh traffic. It resulted in the following /etc/sysconfig/iptables file:
[root@VE /]# cat /etc/sysconfig/iptables
Firewall configuration written by system-config-securitylevel
Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i venet0 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
After that I was able to ssh to VE from HN and from other nodes. But note, that I have no any firewall rules in VE0 (including SNAT/DNAT rules)