Subject: OpenVZ & iptables REDIRECT
Posted by vali.dragnuta on Mon, 15 May 2006 18:32:57 GMT
View Forum Message <> Reply to Message

Hello all,

It seems that I am not the first complaining about iptables REDIRECT + openvz.

My problem follows :
Initially I tried to use REDIRECT inside a VPS to redirect a privileged port to a nonprivileged one (ex : 25 towards 10025 where a certain server listens). Effect : packets get in (tcpdump inside the VPS sees the packets, but nothing gets back. Packets returning can be clearly seen if a connection is initiated directly to the nonprivileged port. The only iptables rule loaded (both in the VPS and in the HOST) is the redirect RULE in the VPS, so accidental filtering is excluded.
After this failed experiment I tried something different : REDIRECT directly on the host OS. In this case the effect is even weirder : it behaves like the rule does not exist at all, for example :
iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
REDIRECT tcp -- anywhere 192.168.12.50 tcp dpt:10022 redir ports 22

...
telnet 192.168.X.X
telnet: Unable to connect to remote host: Connection refused

...even more interesting : the rule does not catch any packet.
iptables -t nat -L -vn
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 REDIRECT tcp -- * * 0.0.0.0/0 192.168.12.50 tcp dpt:10022 redir ports 22

...and even more interesting is that on the VPS the rule catches the packets (rule pkt counter is > 0 on the VPS).

My OS :
Centos 4.3, kernel (both host & vps )
2.6.8-022stab072.2-smp

Am I missing something ? Should I file a bug ? Can anyone confirm this behaviour ?

Thank you very much.

Subject: Re: OpenVZ & iptables REDIRECT
Posted by dim on Tue, 16 May 2006 07:56:40 GMT
View Forum Message <> Reply to Message

Check that you have `options ip_conntrack ip_conntrack_enable_ve0=1` in your /etc/modprobe.conf

Subject: Re: OpenVZ & iptables REDIRECT
Posted by vali.dragnuta on Tue, 16 May 2006 11:57:28 GMT
View Forum Message <> Reply to Message

It is, but does not solve the problem. In fact that module should not even accept parameters. And DNAT (which also needs conntrack) works perfectly inside the VPS, so it must be the REDIRECT implementation, or at least this is what I think, considering the facts above and that REDIRECT does not work on the host node itself,either.

Anyway, I have already reported a bug for this issue, so for anyone interested about this problem - check
http://bugzilla.openvz.org/show_bug.cgi?id=171