Subject: *SOLVED* iptables state in VE broken
Posted by dlzinc on Sat, 30 Jun 2007 00:56:15 GMT
View Forum Message <> Reply to Message

uname -r
2.6.18-8.1.4.el5.028stab035.1

Host is CentOS 5 x86_64
VE is also CentOS 5 x86_64

If I do:
iptables -F
iptables -A INPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -P DROP

I would expect to be able to SSH into this VE, however I can't. Using vzctl enter, I saw the counters for DROP incremented and the single iptables line counter is still 0. There also is no /proc/net/ip_conntrack present inside the VE.

IPTABLES (in the ve .conf file) is not set, all other modules appear to work (e.g. ipt_owner)

conntrack is loaded on the HN and was loaded before the VE was started. Any ideas? or bug...

Oddly enough, I have another box:
2.6.18-8.1.4.el5.028stab035.1
Host is CentOS 4 x86_64
VE is also CentOS 4 i686

state tracking works properly (and there's a /proc/net/ip_conntrack in the VE)

Subject: Re: iptables state in VE broken
Posted by dlzinc on Sat, 30 Jun 2007 01:19:11 GMT
View Forum Message <> Reply to Message

Hrm.. solved it.
Had to do vzctl set [veid] --save --iptables ipt_conntrack --iptables ipt_state etc.

Which is weird, because the docs (man vzctl) say that if the module is loaded (it was) then I shouldn't have to do that.

Subject: Re: iptables state in VE broken
Posted by rickb on Sat, 30 Jun 2007 06:45:42 GMT
View Forum Message <> Reply to Message

it might be loaded but is it configured to be granted to the VE? vz.conf

Subject: Re: iptables state in VE broken
Posted by dlzinc on Sat, 30 Jun 2007 13:17:46 GMT
View Forum Message <> Reply to Message

On the CentOS 4 HN+VE, there is no IPTABLES entry in the veid.conf file and it works fine. On the CentOS 5 HN+VE, it doesn't work without the IPTABLES entry. They're both using the same kernel and same vzctl...

Subject: Re: iptables state in VE broken
Posted by rickb on Sat, 30 Jun 2007 21:17:28 GMT
View Forum Message <> Reply to Message

like I said already, is the IPTABLES bash array in vz.conf identical among your nodes which act differently? this would explain the situation you presented.

Subject: Re: iptables state in VE broken
Posted by dlzinc on Sun, 01 Jul 2007 03:45:11 GMT
View Forum Message <> Reply to Message

Like I said, yes.

The lack of an IPTABLES entry on the CentOS 4 HN+VE = I get /proc/net/ip_conntrack, while the lack of an IPTABLES entry on CentOS 5 HN+VE = I don't get /proc/net/ip_conntrack, however if I *do* add an IPTABLES entry it works fine. The manpage for vzctl states that if there aren't any restrictions (i.e. no IPTABLES entry) then all loaded modules are enabled (which on CentOS 5, doesn't appear to be the case).

Subject: Re: iptables state in VE broken
Posted by rickb on Sun, 01 Jul 2007 04:11:47 GMT
View Forum Message <> Reply to Message

but you are referring to, or at least you said, veid.conf. I said vz.conf. different files. anyway, good luck.

Subject: Re: iptables state in VE broken
Posted by dlzinc on Sun, 01 Jul 2007 16:45:43 GMT
View Forum Message <> Reply to Message

Sorry, misread your post... you're right.

Seems like another admin changed vz.conf from the default on the CentOS 4 box and neglected to document it...