Subject: *SOLVED* Masquerade and OVZ in IPCOP ?
Posted by gwondaleya on Wed, 18 Oct 2006 17:02:53 GMT
View Forum Message <> Reply to Message

Hello,

I own an old box (p2 266, yes i know it 's really old, but wattage is below 50W) on which i perform firewalling using IPCOP.
I want to host on the same machine a web server (yes i know it is not a so good idea, but i have only this box for hosting and can't afford to have two computer running).

i have choosed to be "secure "to use a kernel with virtualization using openvz. i have succesfully "upgraded" the kernel of the ipcop to 2.6.16-026test18 with all the vzctl utils and so on.
i am able to perform all the filtering etc with iptables on the host (hardware node) except the following commands which ends up with : invalid argument, i don't know why

iptables -t nat -A REDNAT -o eth2 -j MASQUERADE
and also:
iptables -t nat -A POSTROUTING -m mark --mark 1 -j SNAT \
        --to-source xx.yy.zz.ww

FYI iptables V1.2.11
Is there someone her which can help me?

Thanks a lot
Jo

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by Valmont on Wed, 18 Oct 2006 17:14:26 GMT
View Forum Message <> Reply to Message

What show these commands?
#iptables -nvL
#iptables -t nat -nvL
#lsmod | grep -i ip

updated:
just one dumb q: Where you try to setup it? On HN or vps?

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by gwondaleya on Wed, 18 Oct 2006 21:29:00 GMT
View Forum Message <> Reply to Message

Hello Valmont,

The commands show these info (see attached files).
It is indeed on the HN node.

In the mean time, i have tried various things related to masquerading and nat, and it seems that i obtain always the same message invalid argument!
It seems tha the module ipt_MASQUERADE is not used in the lsmod listing, while with a "normal" kernel (the ipcop kernel) all works fine and the ipt_MASQUERADE is used OK
Ah i have also tried to set the ip_conntrack_enbale_ve0 option to 1 (even if i know that the kernel 2.6.16 test 18 is already compiled with the support)

What i should try is use a recent iptable binary to see if it works OK or not! And if it doesn't work then...??

Cheers
Jo

File Attachments

1) echo1, downloaded 388 times
2) echo2, downloaded 367 times
3) echo3, downloaded 343 times

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by gwondaleya on Wed, 18 Oct 2006 21:59:27 GMT
View Forum Message <> Reply to Message

Hello,

seems that iptables 1.3.5 (from slackware distrib) is OK for the job and do not produce the error !!
Have to check that thoroughly now, to see if my ipcop box is OK and work ok with a guest

The drawback is that this new iptable binary doesn't seems to work OK with the old kernel....
Have to make a "nice" package of the mods i made on the ipcop to get the thing working and document it.
I know that this solution is not as "nice" as having a true DMZ server and a firewall, but well, for a personal web server/firewall, it is an economic way of doing, with a rather good security (attack of the web site should be contained in the guest domains...i hope) instead of all-in-one firewall/mail/web servers

Another way (more secured ?) is probably to have an ipcop running in a guest, and web/mail/dns in other(s) guest(s), but so far i have been unable to "guest-ify" the ipcop distrib..doesn't want to start....

Thanks for helps

Jo

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by dev on Thu, 19 Oct 2006 08:18:11 GMT
View Forum Message <> Reply to Message

please give me to know if it works now. It is really strange, at least we were unaware of any incompatibilities in iptables<->kernel.

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by gwondaleya on Thu, 19 Oct 2006 13:45:00 GMT
View Forum Message <> Reply to Message

Hello

Yes works now, but with the updated iptable.
Yes it is strnage to me too, since the same iptable version and the latest ovz kernel, on another machine (Mdk community) do not show the error.
Another question, OOT:
Since i have changed to the ovz kernel and all other stuff with iptable in my ipcop box, one of my script showing the connections stop working. the reason is that /proc/net/ip_conntrack is not readable by other, and i am unable to make it readable by other or to change any permission on it (as root)
is there a way to tell to make this file readable by other (ugo+r)?

Thanks
Jo

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by dev on Thu, 19 Oct 2006 13:55:07 GMT
View Forum Message <> Reply to Message

AFAICS, it has access rights 0440 in all kernels.
Why do you need to make this file readable for "other"?
You can patch net/ipv4/netfilter/ip_conntrack_standalone.c file to change 0440 to 0444.

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by gwondaleya on Thu, 19 Oct 2006 14:00:03 GMT
View Forum Message <> Reply to Message

Thanks for the tips .
I want to make it readable by "other" because there is a web script in ipcop which acces this file to get information on what is connected, to which interface etc..
but well , it is not very "important" for now.

Thanks alot.

Subject: Re: Masquerade and OVZ in IPCOP ?
Posted by dev on Thu, 19 Oct 2006 14:11:03 GMT
View Forum Message <> Reply to Message

you are welcome!
I will mark this thread as *SOLVED* for now, so feel free to create a new one if needed and ask any questions.