Subject: [solved] iptables and multiport modul in openvz
Posted by nicolas_79 on Sat, 14 Nov 2009 19:33:37 GMT
View Forum Message <> Reply to Message

Hi Everyone!

i have a problem using the multiport module within an openvz container.

hope someone can help me out!

problem description:

when using the multiport module within a openvz container, i get an error. all other options/modules work fine.

the command also works fine on the host itself!

>iptables -t mangle -A OUTPUT -p tcp -m tcp -m multiport -d 192.168.22.4 --dports 3307,3306 -j Out_RULE_2

returns
FATAL: Could not load /lib/modules/2.6.26-2-openvz-amd64/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.26-2-openvz-amd64/modules.dep: No such file or directory

>iptables -t mangle -A OUTPUT -p tcp -m tcp -j Out_RULE_2

works out fine

ANY IDEAS?

container system (Debian)

>cat /proc/net/ip_tables_matches
udplite
udp
tcp
conntrack
conntrack
state
length
ttl
tcpmss
icmp

multiport
multiport
limit
tos
tos
dscp

host sytem (Debian)

Linux server05 2.6.26-2-openvz-amd64 #1 SMP Wed Aug 19 23:15:49 UTC 2009 x86_64 GNU/Linux

/etc/vz/vz.conf
IPv4 iptables kernel modules
IPTABLES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state iptable_nat ip_nat_ftp"

>cat /proc/net/ip_tables_matches
udplite
udp
tcp
conntrack
conntrack
state
length
ttl
tcpmss
icmp
multiport
multiport
limit
tos
tos
dscp

>lsmod
lsmod
Module Size Used by
vzethdev 14720 0
vznetdev 24456 2
simfs 8944 1
vzrst 123048 0

```
vzcpt                106424  0
tun                  15492  2 vzrst,vzcpt
vzdquota             42868  1 [permanent]
vzmon                31376  5 vzethdev,vznetdev,vzrst,vzcpt
vzdev                7568  4 vzethdev,vznetdev,vzdquota,vzmon
acpi_cpufreq         11792  7
cpufreq_userspace    8452  0
cpufreq_ondemand     11792  1
cpufreq_conservative 11784  0
cpufreq_powersave    6400  0
cpufreq_stats        9120  0
xt_tcpudp            7680  20
nf_conntrack_ipv6    22632  0
ipv6                 296384  52 vzrst,vzcpt,vzmon,nf_conntrack_ipv6
nf_conntrack_proto_dccp 11916  0
nf_conntrack_tftp    9748  0
ts_kmp               6272  5
nf_conntrack_amanda  8832  0
nf_conntrack_netlink 20864  0
nfnetlink            8904  1 nf_conntrack_netlink
nf_conntrack_pptp    10756  0
nf_conntrack_sip     23972  0
nf_conntrack_sane    9764  0
nf_conntrack_netbios_ns 7040  0
nf_conntrack_proto_sctp 12428  0
nf_conntrack_proto_udplite 8844  0
nf_conntrack_proto_gre 9472  1 nf_conntrack_pptp
xt_conntrack         8704  0
nf_conntrack_irc     10680  0
nf_conntrack_h323    57168  0
nf_nat_ftp           7296  0
nf_conntrack_ftp     12728  1 nf_nat_ftp
iptable_nat          11652  1
nf_nat               22548  3 nf_conntrack_netlink,nf_nat_ftp,iptable_nat
xt_state             6656  46
xt_length            6400  0
ipt_ttl              6144  0
xt_tcpmss            6656  0
xt_TCPMSS            8576  0
iptable_mangle       8704  1
iptable_filter       8320  2
ip_tables            21776  3 iptable_nat,iptable_mangle,iptable_filter
xt_multiport         7424  5
xt_limit             7172  0
nf_conntrack_ipv4    24352  51 iptable_nat,nf_nat
nf_conntrack         82688  21 <snipped content>
ipt_LOG              10372  6
xt_DSCP              7808  0
```

```
xt_dscp              7168  0
ipt_REJECT           7552  2
x_tables            25736  15 <snipped content>
loop                19340  0
wmi                 11712  0
snd_pcm             81928  0
snd_timer           25744  1 snd_pcm
i2c_i801            13596  0
snd                 63688  2 snd_pcm,snd_timer
soundcore           12064  1 snd
button              11680  0
snd_page_alloc      13072  1 snd_pcm
i2c_core            27936  1 i2c_i801
pcspkr              7040  0
evdev               14208  0
ext3               124816  2
jbd                 51240  1 ext3
mbcache             12804  1 ext3
dm_mirror           20608  0
dm_log              13956  1 dm_mirror
dm_snapshot         19400  0
dm_mod              58864  3 dm_mirror,dm_log,dm_snapshot
r8169               31492  0
ehci_hcd            36108  0
uhci_hcd            25760  0
sd_mod              29376  8
thermal             22688  0
fan                 9352  0
freq_table          9344  3 acpi_cpufreq,cpufreq_ondemand,cpufreq_stats
processor           42304  10 acpi_cpufreq,thermal
thermal_sys         17728  3 thermal,fan,processor
raid10              23680  0
raid456             125728  0
async_xor           8448  1 raid456
async_memcpy        6912  1 raid456
async_tx            11764  3 raid456,async_xor,async_memcpy
xor                 9744  2 raid456,async_xor
raid1               24192  3
raid0               10624  0
md_mod              80036  7 raid10,raid456,raid1,raid0
atiixp              8324  0 [permanent]
ahci                33036  6
sata_nv             28680  0
sata_sil            13192  0
sata_via            13060  0
libata             165600  4 ahci,sata_nv,sata_sil,sata_via
dock                14112  1 libata
via82cxxx           12164  0 [permanent]
```

```
ide_core              128156  2 atiixp,via82cxxx
3w_9xxx                34948  0
3w_xxxx                28064  0
scsi_mod              161144  4 sd_mod,libata,3w_9xxx,3w_xxxx
```

Subject: Re: iptables and multiport modul in openvz
Posted by nicolas_79 on Mon, 16 Nov 2009 15:58:49 GMT
View Forum Message <> Reply to Message

ok, i found the solution.

depmod -a

recreates the required files in the module directory. after that everything worked out fine.

Subject: Re: iptables and multiport modul in openvz
Posted by fernandomm on Tue, 17 Nov 2009 23:54:13 GMT
View Forum Message <> Reply to Message

Hello,

I am having the same problems that you are having but when starting APF firewall.

Did you run depmod -a on the host server?

I have this on vz.conf:

[code]IPTABLES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state iptable_nat ip_nat_ftp"[code]

My container is also a Debian.

The strange thing is that APF works on containers running CentOS.

Subject: Re: iptables and multiport modul in openvz
Posted by nicolas_79 on Wed, 18 Nov 2009 08:22:28 GMT
View Forum Message <> Reply to Message

Hi fernandomm,

fernandomm wrote on Tue, 17 November 2009 18:54
Did you run depmod -a on the host server?

You will have to run depmod -a in the container. Probably it will then tell you that the target directory (/lib/modules/2.6.26-2-openvz-amd64/) does not exist. create it as root and then re-run depmod -a. iptables should then work with all loaded modules.

fernandomm wrote on Tue, 17 November 2009 18:54
The strange thing is that APF works on containers running CentOS.

as far as i can see the problem lies in the fact that the depmod file was not created in the debian template / container. this probably is based on the fact that this module dependency file normally is created when the kernel image is installed. as this is not necessary when using openvz it has to be done manually and is not described in the "debian template creation instructions" found in the wiki.

Since it works out for CentOS i could imagine that either the CentOS template contained this informations already (perhaps it was a preconfigured download) or something similar.

best regards

nicolas

Subject: Re: iptables and multiport modul in openvz
Posted by fernandomm on Wed, 18 Nov 2009 11:01:34 GMT
View Forum Message <> Reply to Message

Thanks a lot. That did the trick
