Subject: The problem of iptables on FC4
Posted by PondRicefied on Sun, 19 Feb 2006 01:35:03 GMT
View Forum Message <> Reply to Message

I installed ovzkernel-2.6.8-022stab 064.1 on fedora core 4 (Kernel2.6.11).

Then, all accesses came to be denied.
(iptables -P {INPUT and OUTPUT} ACCEPT only is OK)

PLZ help m;;m

The installed step is as follows.

```
--- machine ---
CPU: AMD Athlon(tm) XP 1700+
Memory: 253888k
hda: SAMSUNG SV0602H, ATA DISK drive
/dev/hda2              55G  3.0G   49G   6% /
/dev/hda1              97M   17M   76M  19% /boot
none                  121M     0  121M   0% /dev/shm
/usr/tmpDSK           485M   11M  449M   3% /tmp
/tmp                  485M   11M  449M   3% /var/tmp
---------------
--------------------------------------------
% vi /etc/sysctl.conf

net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 1
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1

% vi /etc/sysconfig/iptables-config

...
IPTABLES_MODULES="ip_tables ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter
iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length"
...

% vi iptables.sh

#!/bin/bash
IPTABLES="/sbin/iptables"
```

```
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
$IPTABLES -F
$IPTABLES -X
$IPTABLES -Z
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
...
$IPTABLES -A INPUT -p tcp -d 123.456.789.012/32 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -s 123.456.789.012/32 -j ACCEPT
...
/etc/init.d/iptables save

% ./iptables.sh
% rpm -Uvh ovzkernel-2.6.8-022stab064.1.i686.rpm
% vi /etc/grub.conf

title OpenVZ (2.6.8-022stab029.1)
        root (hd0,0)
        kernel /vmlinuz-2.6.8-022stab029.1 ro root=/dev/hda2
        initrd /initrd-2.6.8-022stab029.1.img

% rpm -Uvh \
    vzctl-2.7.0-26\
    vzpkg-2.7.0-18\
    vzctl-lib-2.7.0-26\
    vzrpm44-4.4.1-22.5\
    vzyum-2.4.0-11\
    vztmpl-fedora-core-4-2.0-2\
    vzquota-2.7.0-7\
    vzrpm44-python-4.4.1-22.5
% mkdir /vz/template/cache
% cd /vz/template/cache
% wget http://~/fedora-core-4-i386-minimal.tar.gz
% cd /vz/template
% wget http://~/yum-cache-fedora-core-4-i386.tar.gz2
% tar bzvf yum-cache-fedora-core-4-i386.tar.gz2
% chkconfig --add vz
% chkconfig --level 2345 vz on
% reboot

....... console login (because ssh denied) .......
% uname -a

Linux myhost.domain.ltd 2.6.8-022stab064.1 #1 Thu Jan 19 22:16:02 MSK 2006 i686 athlon i386
GNU/Linux
```

```
% ifconfig
eth0   Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
       inet addr:123.456.789.012  Bcast:123.456.789.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       Interrupt:18 Base address:0xd400

lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:1278 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1278 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:180638 (176.4 KiB)  TX bytes:180638 (176.4 KiB)

venet0    Link encap:UNSPEC  HWaddr
XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-XX-X
       UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

% netstat -tua|grep ssh

tcp       0      0 *:ssh  *:*  LISTEN
```

Subject: Re: The problem of iptables on FC4
Posted by dev on Sun, 19 Feb 2006 07:21:47 GMT

View Forum Message <> Reply to Message

I didn't fully got what doesn't work in your case.
First, you have the following rules in your iptables.sh

```
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
...
$IPTABLES -A INPUT -p tcp -d 123.456.789.012/32 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp -s 123.456.789.012/32 -j ACCEPT
```

which means that only 123.456.789.012/32 subnetwork should work fine.

Next, VPS networking requires IP forwarding, so it won't work with this rule:
$IPTABLES -P FORWARD DROP

Also, I would notice, that by default in OVZ kernel conntracks are disabled in host system. This is done so for performance reasons (no double conntracking). But if really needed you can enable it by:
/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"

Subject: Re: The problem of iptables on FC4
Posted by PondRicefied on Sun, 19 Feb 2006 16:19:59 GMT
View Forum Message <> Reply to Message

> Next, VPS networking requires IP forwarding, so it won't work with this rule:
> $IPTABLES -P FORWARD DROP
It was NG even if I changed FORWARD into ACCEPT.

I was doing one wrong guess.
"iptables -A {INPUT,OUTPUT} -{d,s} XXXX.XXXX.XXXX.XXXX -j ACCEPT"
was able to access.
But, I cannot access in "iptables -A {INPUT,OUTPUT} -{d,s} XXXX.XXXX.XXXX.XXXX -m state --state {NEW,ESTABLISHED,RELATED} -j ACCEPT".

I am using the following in the syntax of iptables.
Parameter :
  protocol
  source
  destination
  jump
  in-interface
  out-interface
Matching option :
  icmp
  limit
  multiport
  owner
  state
  tcp
  tos
  ttl
  udp
Expansion of a target :
  LOG
  REJECT

Which should I load in IPTABLES_MODULE (/etc/sysconfig/iptables-config) and IPTABLES (/etc/sysconfig/vz)?

And other configurations. PLZ.

Subject: Re: The problem of iptables on FC4
Posted by dev on Sun, 19 Feb 2006 19:31:36 GMT
View Forum Message <> Reply to Message

As I wrote you need to enable conntracks in host system (VE0) by the following command:
/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"

Subject: Re: The problem of iptables on FC4
Posted by PondRicefied on Sun, 19 Feb 2006 19:51:44 GMT
View Forum Message <> Reply to Message

I have already written it.

```
-- lsmod|grep ip ----------------------
ipt_state              1632  119
ipt_length             1504  1
ipt_ttl               1632  1
ipt_tcpmss             1920  1
ipt_TCPMSS             3648  1
ipt_multiport          1760  1
ipt_limit              1952  24
ipt_tos               1408  1
ipt_REJECT             5536  8
ip_conntrack_ftp      71184  1
iptable_mangle         4256  0
ipt_LOG               6112  28
iptable_filter         4096  2
ipt_MASQUERADE         2176  5
iptable_nat           25916  2 ipt_MASQUERADE
ip_conntrack          35592  5 ipt_state,ip_conntrack_ftp,ipt_MASQUERADE,iptable_nat
ip_tables             20656  14  ipt_state,ipt_length,ipt_ttl,ipt_tcpmss,ipt_TCPMSS,ipt_multi
port,ipt_limit,ipt_tos,ipt_REJECT,iptable_mangle,ipt_LOG,ipt
able_filter,ipt_MASQUERADE,iptable_nat
-------------------------------------
```

Uhmmmm....Why???

Subject: Re: The problem of iptables on FC4
Posted by dev on Sun, 19 Feb 2006 20:04:04 GMT

View Forum Message <> Reply to Message

I'm sorry, can you be more concrete in your messages?
do you have something in this output?
# cat /proc/net/ip_conntrack

Most likely, you need to add the line
/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"
somewhere in your init scripts and reboot the machine.
Or remove this module and then reload with the option provided.
I guess that you simply did modprobe when module is already loaded, in this case modprobe reports the success but does nothing.

Subject: Re: The problem of iptables on FC4
Posted by PondRicefied on Sun, 19 Feb 2006 20:46:51 GMT

View Forum Message <> Reply to Message

> do you have something in this output?
> # cat /proc/net/ip_conntrack

No such file or directory

# ls /proc/net/ip_*
/proc/net/ip_tables_matches
/proc/net/ip_tables_targets
/proc/net/ip_tables_names

> /sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"

I wrote modprobe to /etc/init.d/iptables file and reboot.
but, not accept.

Subject: Re: Re: The problem of iptables on FC4
Posted by dev on Mon, 20 Feb 2006 07:51:20 GMT

View Forum Message <> Reply to Message

>>do you have something in this output?
>># cat /proc/net/ip_conntrack
> No such file or directory
exactly! this means thay ip_conntrack module was loaded without the
option I provided to you.

> # ls /proc/net/ip_*
> /proc/net/ip_tables_matches
> /proc/net/ip_tables_targets

> /proc/net/ip_tables_names
>
>
>>/sbin/modprobe ip_conntrack "ip_conntrack_enable_ve0=1"

> I wrote modprobe to /etc/init.d/iptables file and reboot.
> but, not accept.

probably it is executed too late. And ip_conntrack module is loaded somewhere else, maybe indirectly via loading some other conntrack-dependant module.

Kirill

Subject: Re: Re: The problem of iptables on FC4
Posted by kir on Mon, 20 Feb 2006 07:59:02 GMT

View Forum Message <> Reply to Message

Kirill Korotaev wrote:

>> I wrote modprobe to /etc/init.d/iptables file and reboot.
>> but, not accept.
>
> probably it is executed too late. And ip_conntrack module is loaded
> somewhere else, maybe indirectly via loading some other
> conntrack-dependant module.

Let me give you my $0.02 :)

To provide any parameter on module loading, the best place would be /etc/modprobe.conf file. In our case, to enable connection tracking for the host system, add the following line to /etc/modprobe.conf:

```
options ip_conntrack ip_conntrack_enable_ve0=1
```

After that, you need to reload the module, i.e.

```
modprobe -r ip_conntract
(check that module was really unloaded: /sbin/lsmod | grep conntr)
modprobe ip_conntrack
```