
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
iptables_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 bzf 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-XX
      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
```

```
-----
```