
Subject: *SOLVED* iptables

Posted by [goeldi](#) on Fri, 23 Jun 2006 06:42:12 GMT

[View Forum Message](#) <> [Reply to Message](#)

When I start iptables on my host system, I can no more connect with ssh. Stopping iptables is no option. Can anybody provide a working /etc/sysconfig/iptables file please?

On the host system I already loaded these modules:

```
iptable_filter iptable_mangle ipt_limit ipt_multiport ipt_tos ipt_TOS ipt_REJECT ipt_TCPMSS
ipt_tcpmss ipt_ttl ipt_LOG ipt_length ip_contrack ip_contrack_ftp ip_contrack_irc ipt_contrack
ipt_state ipt_helper iptable_nat ip_nat_ftp ip_nat_irc ipt_REDIRECT
```

The host is CentOS 4.3 with Kernel 2.6.8-022stab077.1 and the vps is CentOS too.

This is the /etc/sysconfig/iptables file:

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
# the following 3 lines I added manually, but I think they do the same as the above ones:
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 19150 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
```

```
COMMIT
# Completed
# Generated by webmin
*nat
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
```

This is the file /etc/sysctl.conf:

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 0
# Enables source route verification
net.ipv4.conf.all.rp_filter = 1
# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 1
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
```

Subject: Re: iptables

Posted by [Vasily Tarasov](#) on Fri, 23 Jun 2006 06:50:06 GMT

[View Forum Message](#) <> [Reply to Message](#)

Just for clarity:

- 1) You can't connect to VPS or to Host?
- 2) iptables rules you've posted are for host or for VPS?

Thanks.

Subject: Re: iptables

Posted by [goeldi](#) on Fri, 23 Jun 2006 06:59:42 GMT

[View Forum Message](#) <> [Reply to Message](#)

hello again

I can't connect to the host (the hardware node) if iptables is loaded with openvz-kernel. I can if iptables is loaded with standard CentOS kernel and I can if openvz-kernel runs WITHOUT iptables.

The posted iptables rules are for the host.

Subject: Re: iptables

Posted by [Vasily Tarasov](#) on Fri, 23 Jun 2006 07:32:09 GMT

[View Forum Message](#) <> [Reply to Message](#)

You should load ip_conntrack module with parameter

ip_conntrack_enable_ve0=1 in 2.6.8 kernel.

Here is described how to do it easily:

<http://forum.openvz.org/index.php?t=tree&th=294&mid=1686&&rev=&reveal=>

Subject: Re: iptables

Posted by [goeldi](#) on Fri, 23 Jun 2006 08:01:09 GMT

[View Forum Message](#) <> [Reply to Message](#)

Yes, that was it. Thank you very much.

Another question though: the w command doesn't show any user logged in in the host and in the vps although there are 2. Is this a openvz or a kernel 2.6.8 'feature'?

Subject: Re: iptables

Posted by [Vasily Tarasov](#) on Fri, 23 Jun 2006 08:10:29 GMT

[View Forum Message](#) <> [Reply to Message](#)

You know, w uses utmp file and /proc as the source of information, and there are lot of nuances... manpage on utmp is interesting =>

You can also check this conversation:

<http://forum.openvz.org/index.php?t=tree&th=413&mid=2373&&rev=&reveal=>
