Subject: IPtables on Centos 4.2 (host system)
Posted by kenchua on Sun, 16 Apr 2006 16:27:20 GMT

View Forum Message <> Reply to Message

Hi

I just downloaded openvz and installed on my CentOS 4.2. But whenever i rebooted my server (iptables started by default), I am unable to access the server remotely. Once IPtables is stopped, I am able to access it.

My question is how do I configure IPtables to enable me to access the server as well as doing IP filtering?

Basically, I wanted to block SMTP, POP3, FTP and HTTP from the host system as it is just supposed to be a "skeleton" for the VPS.

I only wanted to allow SSHD access via 2 static IP addresses used by my company.

Can any gurus please assist me? Thanks

cheers
Ken

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by dim on Mon, 17 Apr 2006 08:19:28 GMT

View Forum Message <> Reply to Message

Seems, that you have to add "options ip_conntrack ip_conntrack_enable_ve0=1" to your /etc/modprobe.conf
After that, restart iptables.

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by kenchua on Sun, 23 Apr 2006 11:34:31 GMT

View Forum Message <> Reply to Message

hi Dim,

thanks for your kind suggestion and it worked

I have another queston. In the VPS, I tried to use lokkit to configure the IPtables and when I restarted IPtables, it reported errors.

Do you have a sample IPtables ruleset for VPS?

Best regards

Ken

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by dev on Mon, 24 Apr 2006 06:57:36 GMT

View Forum Message <> Reply to Message

I'm not sure what lokkit is (probably some frontend for iptables?)...
Maybe you can provide some messages on how it failed?
Also, check that you enabled iptables inside VPS.
default iptable modules available in VPS are listed in /etc/sysconfig/vz, variable IPTABLES.
list of available modules can be found in vzctl man.

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by dowdle on Mon, 24 Apr 2006 22:40:39 GMT

View Forum Message <> Reply to Message

lokkit is Red Hat's tui app for create /etc/sysconfig/iptables. Whenever lokkit is run, it overwrites the previous iptables config with the new info... ie you can't modify an existing file with additional info... as it makes a new config from scratch each time... or at least that is my understanding.

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by kenchua on Thu, 27 Apr 2006 18:12:22 GMT

View Forum Message <> Reply to Message

Hi

I copied the IPTABLES from the host node and tried to use it on the vps. It prompted the error below. Attached is the set of rules for IPTABLES.

```
[root@webvps ~]# /etc/init.d/iptables restart
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: mangle filter             [  OK  ]
Applying iptables firewall rules: iptables-restore: line 17 failed
                                                           [FAILED]


[root@webvps ~]# cat /etc/sysconfig/iptables
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
```

```
:RH-Firewall-1-INPUT - [0:0]
-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 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Subject: Re: IPtables on Centos 4.2 (host system)
Posted by Vasily Tarasov on Fri, 28 Apr 2006 07:22:45 GMT

View Forum Message <> Reply to Message

kenchua,

You didn't add enought iptables modules inside VPS.
Just append to /etc/sysconfig/vz or to /etc/sysconfig/vz-scipts/<VPS-ID>.conf file the string:

```
IPTABLES="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_conntrack ip_conntrack_ftp
ip_conntrack_irc ipt_conntrack ipt_state ipt_helper iptable_nat ip_nat_ftp ip_nat_irc
ipt_REDIRECT"
```

And start-stop VPSs.
This will add ALL iptables modules to VPS.
You can play further with IPTABLES parameter and investigate,
wich of modules are sufficient for you...