Subject: *SOLVED* firewalls for vps.
Posted by sanjooz_2002 on Wed, 06 Dec 2006 08:33:10 GMT
View Forum Message <> Reply to Message

Hi,

I have successfuly installed OpenVZ on centos 4.2. I have also created four virtual servers on this hardware node. I am using quicktables as a firewall on the main hardware node. I wish to configure a firewall on each of the vps es. Unfortunately Quicktables doesnt recognize venet0 as a valid name for a network interfc. Hence, I am not able to use it for my virtual servers.
I wanted to block all the ports except 22,80 and 443 on each of the virtual servers. Can anyone help me?? Thanks in advance!!

Subject: Re: firewalls for vps.
Posted by dim on Wed, 06 Dec 2006 09:12:32 GMT
View Forum Message <> Reply to Message

The best way is to modify quicktables script (most probably, it is rc.firewall in your virtual servers). Just add `venet' in list of the recognized devices.
Something like this:

```
 --- /usr/local/sbin/rc.firewall.ovz       2003-09-02 08:04:54.000000000 +0400
+++ /usr/local/sbin/rc.firewall   2006-12-06 12:08:45.000000000 +0300
@@ -53,7 +53,7 @@ date=`date '+%Y.%m.%d.%S'`

 ### define regex for ip and interface validation ###
 is_ip="grep -Ec
'^[1-2]?[0-9]?[0-9]\.[0-2]?[0-9]?[0-9]\.[0-2]?[0-9]?[0-9]\.[0-2]?[0-9]?[0-9](\/[0-3]?[0-9])?$'"
-is_if="grep -Ec '^(eth|ppp|wlan|tun)[0-9]$'"
+is_if="grep -Ec '^(eth|venet|ppp|wlan|tun)[0-9]$'"

 ### don't overwrite existing output file if present ###
 if [ -f $out ]; then
```

Subject: Re: firewalls for vps.
Posted by sanjooz_2002 on Wed, 06 Dec 2006 10:59:32 GMT
View Forum Message <> Reply to Message

Hi dim,

Thx for the help. I tried whatever you had suggested. Now it gives me the following output when I try running the rc.firewall script.

##################OUTPUT###################################

setting global variables

applying general security settings to /proc filesystem

/usr/src/quicktables-2.3/rc.firewall: line 16: /proc/sys/net/ipv4/tcp_syncookies: Operation not permitted
iptables: No chain/target/match by that name
applying icmp rules

iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
applying the open port(s) to the firewall rules

applying default drop policies

quicktables is loaded

Now I have no internet connectivity from within my vps. I cant even ping other machines on the local network. I had to restart the vps inorder to restore the previous settings. Can you tell me as to what the error means? Thanks once again!!

cheers'

Subject: Re: firewalls for vps.
Posted by sanjooz_2002 on Wed, 06 Dec 2006 11:01:49 GMT
View Forum Message <> Reply to Message

Or is there any other open source software that would serve my needs. .i.e block all ports other than 22,80 and 443 on the vps.

Thanks!

Subject: Re: firewalls for vps.
Posted by dim on Wed, 06 Dec 2006 11:22:11 GMT
View Forum Message <> Reply to Message

You need to know which iptables modules are required by your script and permit them for this VE.
Seems, that the fastest way to resolve the issue will be access to your node.
Could you give me such access (via PM, of course)?

Subject: Re: firewalls for vps.
Posted by sanjooz_2002 on Thu, 07 Dec 2006 10:27:37 GMT
View Forum Message <> Reply to Message

Hi dim,

Well, I have solved the main problem .i.e the loading of modules. I just edited the IPTABLES line in the /etc/sysconfig/vz file. Now it looks something like this:

IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ip_conntrack ip_conntrack_ftp ip_conntrack_irc ipt_LOG ipt_conntrack ipt_helper ipt_state iptable_nat ip_nat_ftp ip_nat_irc ipt_TOS"

!!!I know I have loaded all the modules and I am not sure if that is a good idea. But, anyways it has solved my problem partially. I have tried accessing a blocked port on my vps and as desired it was inaccessible. Now when I run the rc.firewall script I get the following output
##
setting global variables

applying general security settings to /proc filesystem

/usr/src/quicktables-2.3/rc.firewall: line 16: /proc/sys/net/ipv4/tcp_syncookies: Operation not permitted
applying icmp rules

applying the open port(s) to the firewall rules

applying default drop policies

quicktables is loaded

Now, as you can see, the only problem is the /proc/sys/netipv4/tcp_syncookies. After reading through few security related artcicles on the internet I realized that it is meant to thwart SYN attack. I looked at the permission rights for this file. it was 644. I tried changing it but to no avail (although I was logged in as root). I even tried to delete it , but it still says that "operation not permitted". Any ideas on how to deal with this problem??

Thanks!!

cheers;

Subject: Re: firewalls for vps.
Posted by sanjooz_2002 on Thu, 07 Dec 2006 11:55:16 GMT
View Forum Message <> Reply to Message

I have made an error in the previous post. I apologize for the same. The permission rights are not 644. Its 444. .i.e only read permission is given and i believe the rc.firewall script uses a command echo 1 > /proc/sys/net/ipv4/tcp_syncookies.

#ls -ld /proc/sys/net/ipv4/tcp_syncookies
-r--r--r-- 1 root root 0 Dec 7 07:52 /proc/sys/net/ipv4/tcp_syncookies

As you can see the permission rights do not permit the script to write into the file.

Pls help!!
Thanks in advance.

Subject: Re: firewalls for vps.
Posted by dim on Thu, 07 Dec 2006 12:08:17 GMT
View Forum Message <> Reply to Message

This is because it is system-wide variable. So, it's change is prohibited in VEs. Your firewall should work without it. If you don't like this message, just comment out this attempt in the rc.firewall script.

Subject: Re: firewalls for vps.
Posted by sanjooz_2002 on Thu, 07 Dec 2006 12:15:13 GMT
View Forum Message <> Reply to Message

Thanks a lot for your help dim!!!

Just one doubt.If the the value in this file (in the vps) is not changed does it (the vps) become vulnerable to SYN attack??

Thanks!

cheers'

Subject: Re: firewalls for vps.
Posted by dim on Thu, 07 Dec 2006 12:19:30 GMT
View Forum Message <> Reply to Message

It depends on current value, which is setuped from HN itself.