Subject: OpenVZ & Shorewall
Posted by zoom on Mon, 20 Mar 2006 02:33:49 GMT
View Forum Message <> Reply to Message

Just wondering if I need to do something special with Shorewall under OpenVZ? I know on Xen I needed to enable bridging etc. Has anyone had any luck with Shorewall using OpenVZ? I should mention that I'm trying to get it working on the Host, not the VPS'..

Thanks.

Subject: Re: OpenVZ & Shorewall
Posted by kir on Mon, 20 Mar 2006 06:24:23 GMT
View Forum Message <> Reply to Message

I anticipate there should not be any problems really.

Subject: Re: OpenVZ & Shorewall
Posted by zoom on Mon, 20 Mar 2006 20:23:49 GMT
View Forum Message <> Reply to Message

There seems to be a problem somewhere. If I reboot the system and use my original kernel, then start shorewall everything seems fine. However, if I attempt to start shorewall using the OpenVZ kernel it doesn't complete and thus locks me out remotely.. I need to reboot, or shutdown shorewall with 'shorewall clear' in order to connect remotely again..

I know the problem isn't the shorewall settings since it works perfectly under the original kernel.. Initially I though it might be the iptable kernel modules, however I did a comparsion of both the modules loaded using the original kernel vs the OpenVZ kernel..

Both have the following modules enabled.

ipt_length
ipt_ttl
ipt_tcpmss
ipt_TCPMSS
iptable_mangle
iptable_filter
ipt_multiport
ipt_limit
ipt_tos
ipt_REJECT
ip_tables

I know that I can enable addition modules in /etc/sysconfig/iptables-config as per the documentation under advanced tasks ie: iptable_nat etc.. tried that and still nothing.

I'm not doing anything on the Hardware node that's complex, just providing a simple firewall using shorewall.. Any ideas??? anything else I should be checking???

Subject: Re: OpenVZ & Shorewall
Posted by dev on Mon, 20 Mar 2006 20:42:10 GMT
View Forum Message <> Reply to Message

try adding:

```
options ip_conntrack ip_conntrack_enable_ve0=1
```

to /etc/modules.conf

Subject: Re: OpenVZ & Shorewall
Posted by kir on Mon, 20 Mar 2006 20:48:54 GMT
View Forum Message <> Reply to Message

You can write a short script like this:

```
F=/tmp/out.ovz
lsmod >> $F
iptables -Ln >> $F
echo "Starting shorewall" >> $F
shorewall start 2>&1 | tee -a $F
echo "Shorewall started" >> $F
lsmod >> $F
iptables -Ln >> $F
echo "Clearing shorewall" >> $F
shorewall clear 2>&1 | tee -a $F
echo "Shorewall cleared" >> $F
lsmod >> $F
iptables -Ln >> $F
```

and run it on openvz box, then change the F and run it on your original kernel. As you see shorewall rules will be cleared so you will have access to the box.

What you do next is compare those two files you get. Run diff -u on them to see the difference (or you could even see some error message from 'shorewall start' command).

If you will still have a problem, post the diff here (as an attachement) and we will take a look.

Regards,
 Kir

Subject: Re: OpenVZ & Shorewall
Posted by kir on Mon, 20 Mar 2006 20:58:53 GMT

View Forum Message <> Reply to Message

Quote:try adding 'options ip_conntrack ip_conntrack_enable_ve0=1' to /etc/modules.conf

Isn't it enabled by default in all the recent kernels, staring from 062 or so? Hmm I am probably wrong - can't find it in changelogs.

Subject: Re: OpenVZ & Shorewall
Posted by zoom on Tue, 21 Mar 2006 00:21:57 GMT

View Forum Message <> Reply to Message

In order to determine what capabilities I have with the original kernel vs the OpenVZ kernel I used the shorewall command "shorewall show capabilities" It seems there are a few differences that could account for it not functioning correctly under the OpenVZ kernel on the Host hardware.

The ones highlighted in Red seem to be missing from OpenVZ.

```
OpenVZ Kernel IPTables Capabilities:
   NAT: Available
   Packet Mangling: Available
   Multi-port Match: Available
   Extended Multi-port Match: Not available
   Connection Tracking Match: Available
   Packet Type Match: Not available
   Policy Match: Not available
   Physdev Match: Not available
   IP range Match: Available
   Recent Match: Available
   Owner Match: Not available
   Ipset Match: Not available
   CONNMARK Target: Not available
   Connmark Match: Not available
   Raw Table: Not available
   CLASSIFY Target: Available

Original Kernel IPTables Capabilities:
   NAT: Available
   Packet Mangling: Available
   Multi-port Match: Available
   Extended Multi-port Match: Not available
   Connection Tracking Match: Available
   Packet Type Match: Available
   Policy Match: Not available
   Physdev Match: Available
   IP range Match: Available
   Recent Match: Available
   Owner Match: Available
   Ipset Match: Not available
   CONNMARK Target: Not available
   Connmark Match: Not available
   Raw Table: Available
   CLASSIFY Target: Available
```

This is what lsmod shows running the OpenVZ kernel.

```
Module                  Size  Used by
ipt_TOS                 2112  0
ipt_state               1632  12
ipt_SAME                2048  0
ipt_recent              9196  0
ipt_NETMAP              1472  0
ipt_MASQUERADE          2176  0
ipt_MARK                1440  0
ipt_mark                1152  0
ipt_mac                 1376  0
ipt_LOG                 6176  9
ipt_iprange             1472  0
ipt_helper              1696  0
ipt_conntrack           2240  0
ipt_CLASSIFY            1536  0
ip_nat_irc              3664  0
ip_nat_tftp             2544  0
ip_nat_ftp              4272  0
iptable_nat            26492  6  ipt_SAME,ipt_NETMAP,ipt_MASQUERADE,ip_nat_irc,ip_nat_tftp,ip
_nat_ftp
ip_conntrack_irc       70416  1 ip_nat_irc
ip_conntrack_tftp       2640  0
ip_conntrack_ftp       71408  1 ip_nat_ftp
ip_conntrack           35688  13
ipt_state,ipt_SAME,ipt_NETMAP,ipt_MASQUERADE,ipt_helper,ipt_
conntrack,ip_nat_irc,ip_nat_tftp,ip_nat_ftp,iptable_nat,ip_c
onntrack_irc,ip_conntrack_tftp,ip_conntrack_ftp
simfs                   3612  2
vzdquota               38576  2 [permanent]
af_packet              16360  0
```

```
ipt_length             1504  2
ipt_ttl                1632  2
ipt_tcpmss             1920  2
ipt_TCPMSS             3648  2
iptable_mangle         4256  3
iptable_filter         4096  3
ipt_multiport          1760  6
ipt_limit              1952  2
ipt_tos                1408  2
ipt_REJECT             5568  6
ip_tables             20656  25  ipt_TOS,ipt_state,ipt_SAME,ipt_recent,ipt_NETMAP,ipt_MASQUER
ADE,ipt_MARK,ipt_mark,ipt_mac,ipt_LOG,ipt_iprange,ipt_helper
,ipt_conntrack,ipt_CLASSIFY,iptable_nat,ipt_length,ipt_ttl,i
pt_tcpmss,ipt_TCPMSS,iptable_mangle,iptable_filter,ipt_multi port,ipt_limit,ipt_tos,ipt_REJECT
parport_pc            23104  1
lp                     7976  0
parport               20544  2 parport_pc,lp
i2c_dev                7872  0
i2c_core              18416  1 i2c_dev
sunrpc               129028  1
vznetdev              12480  5
vzmon                 41632  3 vznetdev
vzdev                  1792  3 vzdquota,vznetdev,vzmon
thermal               10096  0
processor             10244  1 thermal
fan                    2668  0
button                 4408  0
battery                7052  0
asus_acpi              8920  0
ac                     3084  0
usbhid                22240  0
usbmouse               4064  0
uhci_hcd              28656  0
usbcore              100356  5 usbhid,usbmouse,uhci_hcd
3c59x                 34408  0
floppy                54192  0
ide_cd                36800  0
cdrom                 37212  1 ide_cd
```

I believe the problem is the missing items shown in Red. Comments???

THanks./.

Subject: Re: OpenVZ & Shorewall
Posted by dev on Tue, 21 Mar 2006 05:59:46 GMT

View Forum Message <> Reply to Message

zoom,

1. I really believe for a firewall, which should run on different distributions this should not be a problem. Can you describe exactly, what do you do with it, how try to configure it and how it refuses to work? Maybe you can give us an access to your node, so that we checked and resolved it quickly. If so, send me a private message with credentials. If not, it is ok.

2. Actually these modules present in OpenVZ kernel sources, they are just not compiled by default in our binary distribution.

Corresponding to these 4 modules config options are:

```
CONFIG_IP_NF_MATCH_PKTTYPE
CONFIG_IP_NF_MATCH_PHYSDEV
CONFIG_IP_NF_MATCH_OWNER
CONFIG_IP_NF_RAW
```

You can try setting them to 'm', recompile the kernel and check whether it helps. If you are unfamiliar with kernel recompilation procedure, we can describe it to you in more details.

Subject: Re: OpenVZ & Shorewall
Posted by zoom on Wed, 22 Mar 2006 15:37:40 GMT

View Forum Message <> Reply to Message

dev,

First, thanks for your help. I've been fighting with this problem for a couple of days now. The reason I suspect it might be a kernel problem is because the script works fine using the original kernel. I don't believe it has anything to do with my shorewall settings simply because it works fine under that situation.

Anyhow, I tried setting the items you indicated and recompiling the kernel. I did run in a a couple of problems with it. First I tried the simple thing which is just to build a new kernel from it's sources in place.. no changes.

```
rpm -ivh ovzkernel-2.6.8-022stab072.2.src.rpm
rpmbuild -bb --target=i686 /usr/src/redhat/SPECS/kernel-ovz.spec
```

The problem is that in the end I did get an RPM built, however it wasn't what I was expecting. The RPM created in /usr/src/redhat/RPMS was

ovzkernel-debuginfo-2.6.8-022stab072.2.i686.rpm

Am I missing something??

Subject: Re: OpenVZ & Shorewall
Posted by dev on Wed, 22 Mar 2006 20:26:23 GMT
View Forum Message <> Reply to Message

what were the error messages reported by rpmbuild?
Can you post it somewhere?
If needed, I can rebuilt it for you with these options to check...