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./.
