Subject: iptables stop -> kernel panic
Posted by goeldi on Fri, 17 Dec 2010 16:57:06 GMT
View Forum Message <> Reply to Message

This container has 16GB RAM and is running the latest stable 64 bit kernel:

uname -a
Linux grey.goeldi.net 2.6.18-194.26.1.el5.028stab079.1 #1 SMP Sat Nov 27 00:56:10 MSK 2010 x86_64 x86_64 x86_64 GNU/Linux

It has 1 CT (32bit) running. When I stop or restart IPTables either in the node or the container (does not matter) I get the kernel panic. Screenshot and dmesg output is attached.

sysctl.conf:
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 0
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 1
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 68719476736
kernel.shmall = 4294967296

223.conf:
ONBOOT="yes"
KMEMSIZE="42816566:45192970"
LOCKEDPAGES="256:256"
PRIVVMPAGES="3517563:3699650"
SHMPAGES="28620:28620"
NUMPROC="618:618"
PHYSPAGES="0:2147483647"
VMGUARPAGES="33792:2147483647"
OOMGUARPAGES="3885567:2147483647"
NUMTCPSOCK="1636:1636"
NUMFLOCK="188:206"
NUMPTY="16:16"
NUMSIGINFO="256:256"
TCPSNDBUF="4908266:5268080"
TCPRCVBUF="22553341:24206672"
OTHERSOCKBUF="1126080:2097152"
DGRAMRCVBUF="262144:262144"

NUMOTHERSOCK="360:360"
DCACHESIZE="3409920:3624960"
NUMFILE="9312:9312"
AVNUMPROC="180:180"
NUMIPTENT="128:128"
DISKSPACE="20971520:20971520"
DISKINODES="200000:220000"
QUOTATIME="0"
CPUUNITS="250000"
CPUS="2"
CPULIMIT="0"
IP_ADDRESS="192.168.2.23"
HOSTNAME="stage.mediq.ch"
VE_ROOT="/vz/root/$VEID"
VE_PRIVATE="/vz/private/$VEID"
OSTEMPLATE="centos-5-x86"
ORIGIN_SAMPLE="basic"
NAMESERVER="212.40.0.10"
NOATIME="yes"
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
IOPRIO="1"

File Attachments

1) dmesg.txt, downloaded 375 times
2) panic.jpg, downloaded 752 times

Subject: Re: iptables stop -> kernel panic
Posted by goeldi on Sun, 19 Dec 2010 11:20:13 GMT
View Forum Message <> Reply to Message

This looks like an old bug. After some additional testing I can say this:

the kernel panic happens, when unloading IPTables modules (e.g. by restarting or stopping the iptables service).

So I changed /etc/sysconfig/iptables-config from:

IPTABLES_MODULES="ip_conntrack_netbios_ns"
IPTABLES_MODULES_UNLOAD="yes"

to:

IPTABLES_MODULES=""
IPTABLES_MODULES_UNLOAD="no"

Now I can restart/stop/start IPTables in Node and CT without any problem.

What implications will this fix have to my openvz practice?
