Subject: Re: IP Conntrack FTP in VE
Posted by ilass on Sun, 21 Mar 2010 11:50:29 GMT
View Forum Message <> Reply to Message

Confirm.

Using kernel-PAE-2.6.27-kiprensky.1.i686.rpm from official page,
using my distro supplied kernel, my own build using patch-kiprensky.1-combined.gz, i get same result as described. I also tried this on different HW (all x86 platform).

Some info about my system(s)/configs:

Hardware node
uname -m
i686

uname -r
2.6.27-kiprensky.1-PAE

lsmod |egrep '(conn|state)'
xt_state 5896 4
nf_conntrack_ipv4 14104 8 iptable_nat,nf_nat
x_tables 15756 8
ipt_ttl,ipt_REJECT,xt_tcpudp,xt_state,xt_hashlimit,iptable_nat,ip_tables,xt_multiport
nf_conntrack_ftp 11060 0
nf_conntrack 60820 5 xt_state,iptable_nat,nf_nat,nf_conntrack_ipv4,nf_conntrack_ftp

# egrep 'IPTABLES' /etc/vz/conf/1003.conf
IPTABLES="ip_tables iptable_filter iptable_nat iptable_mangle ip_conntrack ip_conntrack_ftp ipt_state ipt_multiport ipt_helper"

On hardware node no iptables rules configured in FORWARD chain and tables 'raw', 'mangle', 'nat'.
Please look at module refcount: it 0, but VE started. On 2.6.18 (production) everything is ok and refcount ~ 18. Is this normal?

VE
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 21,80,873 -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type 8 -m hashlimit --hashlimit-upto 30/sec --hashlimit-mode dstip --hashlimit-name echo_request -j ACCEPT

iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -p udp -m udp --sport 1024:65535 --dport 53

-j ACCEPT

cat /proc/net/ip_tables_matches
ttl
udplite
udp
tcp
state
hashlimit
hashlimit
icmp
multiport
multiport

cat /proc/net/ip_tables_names
mangle
filter

Using same rules on HN i get with working ftp in passive/active (production rules mostly identical), also using

iptables -A FORWARD -m helper --helper ftp -j ACCEPT

on HN, and then connecting to ftp, i see packet count increment for this rule: so nf_conntrack_ftp matches packets. Tcpdump on venet0 also confirms this.
I also try to establish connection from VE to ftp and get same result. Modes tried: passive, active.
