Subject: OpenVZ + OpenVPN + iptables
Posted by gatos on Sat, 07 Oct 2006 21:42:54 GMT
View Forum Message <> Reply to Message

Hello,

I decided to move my OpenVPN into OpenVZ, but I got some troubles. I guess it's NAT. tun0 device doesn't forward any packets TX=0.

iptables rules:

iptables -t nat -A POSTROUTING -j SNAT --to 88.xx.81.85 -s 192.168.2.0/255.255.255.0

tcpdump -i tun0

21:29:47.648984 IP 192.168.2.5 > 64.233.167.99: ICMP echo request, id 1536, seq 20224, length 40
21:29:52.929442 IP 192.168.2.5 > 64.233.167.99: ICMP echo request, id 1536, seq 20480, length 40

/etc/vz/vz.conf
IPTABLES="iptable_nat ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length"

/etc/modprobe.conf

..
options ip_conntrack ip_conntrack_enable_ve0=1

ifconfig

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.15.1  P-t-P:192.168.15.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:3872 (3.7 KiB)  TX bytes:0 (0.0 b)

venet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:127.0.0.1  P-t-P:127.0.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
```

RX packets:706 errors:0 dropped:0 overruns:0 frame:0
TX packets:454 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:61208 (59.7 KiB) TX bytes:58291 (56.9 KiB)

venet0:0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:88.xx.81.85 P-t-P:88.xx.81.85 Bcast:0.0.0.0 Mask:255.255.255.255
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1

Thank you in advance

Subject: Re: OpenVZ + OpenVPN + iptables
Posted by dev on Sun, 08 Oct 2006 17:08:05 GMT
View Forum Message <> Reply to Message

Have you read this article already:
http://wiki.openvz.org/VPN_via_the_TUN/TAP_device
?

try checking log files already.

Subject: Re: OpenVZ + OpenVPN + iptables
Posted by dlzinc on Mon, 09 Oct 2006 04:52:31 GMT
View Forum Message <> Reply to Message

Inside the VE, check if IP forwarding is enabled?
sysctl net.ipv4.ip_forward

To enable:
sysctl net.ipv4.ip_forward = 1

You'll also need routes on the HN to tell it where to send the received NATed packets. (I think that's all you need at least...)

Subject: Re: OpenVZ + OpenVPN + iptables
Posted by gatos on Mon, 09 Oct 2006 10:10:08 GMT
View Forum Message <> Reply to Message

I have done all those steps:
http://wiki.openvz.org/VPN_via_the_TUN/TAP_device
and tun device is being used:
[root@r8c2 ~]# lsmod | grep tun
tun   6880 1

And I was trying to enable debug on iptables:
iptables -t nat -A PREROUTING -j LOG --log-prefix "NAT Prerouting: "
iptables -t nat -A POSTROUTING -j LOG --log-prefix "NAT Postrouting: "
iptables -t nat -A OUTPUT -j LOG --log-prefix "NAT Output: "

but I got a strange error:
iptables: Unknown error 4294967295

Forwarding is set to '1'.
net.ipv4.ip_forward = 1

Subject: Re: OpenVZ + OpenVPN + iptables
Posted by dev on Mon, 09 Oct 2006 11:49:17 GMT
View Forum Message <> Reply to Message

can you give an access to the node to check?

Subject: Re: OpenVZ + OpenVPN + iptables
Posted by dev on Tue, 10 Oct 2006 07:25:15 GMT
View Forum Message <> Reply to Message

1. why have you installed vzctl inside VE?
this makes apg-get install to fail

2. I installed strace inside the VE.

3. I straced openvpn process 13724. You can find output in out and
out.2 files.
out.2 file demonstrates that this process reads ping ICMP packets from /dev/net/tun:
read(6, "E\0\0T\0\0@\0@\1\233U\300\250\17\1\300\250\17\2\10\0Se"..., 1500) = 84

/dev/net/tun has fd=6:
debian-tun-1:~# ls /proc/13724/fd -la
lrwx------ 1 root root 64 Oct 10 07:12 6 -> /dev/net/tun

i.e. tun/tap works fine.

4. however this process doesn't send the packet anywhere...
it looks like it tries to negotiate with the other end:

send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 70, MSG_NOSIGNAL) = 70
send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 79, MSG_NOSIGNAL) = 79
send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 74, MSG_NOSIGNAL) = 74
send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 81, MSG_NOSIGNAL) = 81
send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 81, MSG_NOSIGNAL) = 81
send(4, "<29>Oct 10 07:15:46 ovpn-server["..., 67, MSG_NOSIGNAL) = 67

but gets no reply :/

fd 4:
lrwx------ 1 root root 64 Oct 10 07:12 4 -> socket:[745036]

debian-tun-1:~# netstat -nap
unix 2 [ ] DGRAM 745036 13724/openvpn

5. So I guess your configuration of openvpn is wrong