Subject: vpnc in a VE locks out local traffic ?
Posted by daryn on Fri, 09 May 2008 17:14:51 GMT
View Forum Message <> Reply to Message

Hello,

vpnc 0.5.1 installed on a centos-4-i386-default VE seems to lock out local network traffic when the VPN is established. I can't even ping the VE from the host.

This is before establishing the VPN. The host is 192.168.2.20, and the VE is 192.168.2.101

```
[root@ovhost ~]# uname -a
Linux ovhost 2.6.18-53.1.13.el5.028stab053.10 #1 SMP Tue Apr 1 14:58:47 MSD 2008 i686 i686
i386 GNU/Linux
[root@ovhost ~]# ping -c 3 192.168.2.101
PING 192.168.2.101 (192.168.2.101) 56(84) bytes of data.
64 bytes from 192.168.2.101: icmp_seq=0 ttl=64 time=0.449 ms
64 bytes from 192.168.2.101: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 192.168.2.101: icmp_seq=2 ttl=64 time=0.000 ms

--- 192.168.2.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.000/0.199/0.449/0.187 ms, pipe 2
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
AAA.AAA.0.0     0.0.0.0         255.255.0.0     U     0      0        0 venet0
0.0.0.0         192.0.2.1       0.0.0.0         UG    0      0        0 venet0
[root@ovhost ~]#
```

Now when I establish the VPN :

```
[root@ovhost ~]# vzctl exec 101 /usr/local/sbin/vpnc
VPNC started in background (pid: 9828)...
[root@ovhost ~]# ping 192.168.2.101
PING 192.168.2.101 (192.168.2.101) 56(84) bytes of data.

<killed>

--- 192.168.2.101 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7005ms
```

```
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
CCC.CCC.CCC.CCC 0.0.0.0         255.255.255.255 UH    0      0        0 venet0
DDD.DDD.DDD.DDD 0.0.0.0         255.255.255.255 UH    0      0        0 tun0
EEE.EEE.EEE.EEE 0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
AAA.AAA.0.0     0.0.0.0         255.255.0.0     U     0      0        0 venet0
192.168.0.0     0.0.0.0         255.255.0.0     U     0      0        0 tun0
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 tun0
0.0.0.0         0.0.0.0         0.0.0.0         U     0      0        0 tun0
[root@ovhost ~]# vzctl exec 101 /usr/local/sbin/vpnc-disconnect
Terminating vpnc daemon (pid: 9828)
[root@ovhost ~]#
```

I have run a few scripts and the VPN within the VE seems indeed operational. However I cannot ssh into the VE while the VPN is up. Existing ssh sessions time out.

I have tried installing vpnc in the host and it works like a charm, without locking out local traffic.

What am I missing ?

TIA,

Subject: Re: vpnc in a VE locks out local traffic ?
Posted by maratrus on Fri, 16 May 2008 16:01:29 GMT
View Forum Message <> Reply to Message

Hello,

You haven't provided us with your network configuration but I guess the problem is in the following:

Quote:

```
192.168.0.0     0.0.0.0         255.255.0.0     U     0      0        0 tun0
```

Are you sure that it's what you want? Do you want to communicate with HN via tun0 interface? Why? Try to communicate with HN via venet interface. Does it help?

P.S. You can use "tcpdump" utility to find out if the packets come inside VE and where they go out.

Thank You!

Subject: Re: vpnc in a VE locks out local traffic ?
Posted by daryn on Thu, 22 May 2008 10:07:39 GMT
View Forum Message <> Reply to Message

Hi, thanks for your answer.

Indeed that was the problem and adding a static route to the local network (192.168.2.0/24) prior to starting vpnc solves it :

```
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
0.0.0.0         192.0.2.1       0.0.0.0         UG    0      0        0 venet0
[root@ovhost ~]# vzctl exec 101 route add -net 192.168.2.0 netmask 255.255.255.0 dev venet0
.0 dev venet0
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 venet0
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
0.0.0.0         192.0.2.1       0.0.0.0         UG    0      0        0 venet0
[root@ovhost ~]# vzctl exec 101 /usr/local/sbin/vpnc
VPNC started in background (pid: 32582)...
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
CCC.CCC.CCC.CCC 0.0.0.0         255.255.255.255 UH    0      0        0 venet0
DDD.DDD.DDD.DDD 0.0.0.0         255.255.255.255 UH    0      0        0 tun0
EEE.EEE.EEE.EEE 0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 venet0
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
192.168.0.0     0.0.0.0         255.255.0.0     U     0      0        0 tun0
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 tun0
0.0.0.0         0.0.0.0         0.0.0.0         U     0      0        0 tun0
[root@ovhost ~]# ping -c 3 192.168.2.101
PING 192.168.2.101 (192.168.2.101) 56(84) bytes of data.
64 bytes from 192.168.2.101: icmp_seq=0 ttl=64 time=0.443 ms
64 bytes from 192.168.2.101: icmp_seq=1 ttl=64 time=0.282 ms
64 bytes from 192.168.2.101: icmp_seq=2 ttl=64 time=0.196 ms

--- 192.168.2.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.196/0.307/0.443/0.102 ms, pipe 2
[root@ovhost ~]# vzctl exec 101 ping -c 3 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 56(84) bytes of data.
64 bytes from 192.168.2.20: icmp_seq=0 ttl=64 time=0.682 ms
64 bytes from 192.168.2.20: icmp_seq=1 ttl=64 time=0.695 ms
```

```
64 bytes from 192.168.2.20: icmp_seq=2 ttl=64 time=0.656 ms

--- 192.168.2.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.656/0.677/0.695/0.034 ms, pipe 2
[root@ovhost ~]# vzctl exec 101 ping -c 3 target.host.on.the.vpn
PING target.host.on.the.vpn (XXX.XXX.XXX.XXX) 56(84) bytes of data.
64 bytes from target.host.on.the.vpn (XXX.XXX.XXX.XXX): icmp_seq=0 ttl=62 time=23.5 ms
64 bytes from target.host.on.the.vpn (XXX.XXX.XXX.XXX): icmp_seq=1 ttl=62 time=31.4 ms
64 bytes from target.host.on.the.vpn (XXX.XXX.XXX.XXX): icmp_seq=2 ttl=62 time=32.0 ms

--- target.host.on.the.vpn ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 23.591/29.031/32.099/3.859 ms, pipe 2
[root@ovhost ~]# vzctl exec 101 /usr/local/sbin/vpnc-disconnect
Terminating vpnc daemon (pid: 32582)
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 venet0
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
0.0.0.0         192.0.2.1       0.0.0.0         UG    0      0        0 venet0
[root@ovhost ~]#
```

I am not sure it is the best solution but it does work. I made the route persistent across VE restarts as follows:

```
[root@ovhost ~]# vzctl enter 101
[root@ov101 /]# cat /etc/sysconfig/network-scripts/route-venet0
192.0.2.0/24 dev venet0 scope host
default via 192.0.2.1
[root@ov101 /]# echo 192.168.2.0/24 dev venet0 >> /etc/sysconfig/network-scripts/route-venet0
/route-venet0
[root@ov101 /]# cat /etc/sysconfig/network-scripts/route-venet0
192.0.2.0/24 dev venet0 scope host
default via 192.0.2.1
192.168.2.0/24 dev venet0
[root@ov101 /]# logout
exited from VE 101
[root@ovhost ~]# vzctl restart 101
Restarting VE
Stopping VE ...
VE was stopped
VE is unmounted
Starting VE ...
VE is mounted
```

```
Adding IP address(es): 192.168.2.101
Setting CPU units: 1000
Setting devices
Configure meminfo: 65536
Set hostname: ov101
File resolv.conf was modified
VE start in progress...
[root@ovhost ~]# vzctl exec 101 route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 venet0
192.0.2.0       0.0.0.0         255.255.255.0   U     0      0        0 venet0
0.0.0.0         192.0.2.1       0.0.0.0         UG    0      0        0 venet0
[root@ovhost ~]#
```

Thank you!