
Subject: OpenVZ and IP masquerading
Posted by [Santi](#) on Tue, 18 Apr 2006 11:53:50 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

We have a Debian Sarge box which runs this script to enable NAT/IP masquerading to local network machines:

```
Quote:#!/bin/sh
modprobe iptable_nat
modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -F
iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```

eth0 = Internet
eth1 = LAN

It works fine with Debian's default kernel, "2.6.8-2-386". I have compiled OpenVZ 2.6.8-022stab076-up, with "enterprise" .config file from OpenVZ site, and when booting with this kernel everything works well except NAT/masquerading with the same iptables rules

I have search in this forum a howto to enable Internet access to the VPS, which has this rule:

http://forum.openvz.org/index.php?t=tree&goto=13&#ms_g_13

Quote:
iptables -t nat -A POSTROUTING -s src_net -o eth0 -j SNAT --to ip_address

This rules depends "ip_address" variable, and it's a big problem because our public IP is dinamic, and can change

Why those rules of iptables dont work with OpenVZ kernel? What's the best way to enable NAT/masquerading to my local network? thanks!!

Regards,

--
Santi Saez

Subject: Re: OpenVZ and IP masquerading
Posted by [dev](#) on Wed, 19 Apr 2006 13:45:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

See FAQ issue here:

<http://openvz.org/documentation/faq>

Quote:

Q. My node is unaccessible through the network after reboot...

A. You need to check your firewall rules. The problem is that default stateful firewall rules are not available on the host system. To make this functionality available, load the `ip_conntrack` module with the additional parameter "`ip_conntrack_enable_ve0=1`". However, this method is highly not recommended because tracking all the connection on the host system lead to performance degradation, more memory usage and also may lead to the total server inaccessibility due to reaching of the overall connection limit.

In latests kernels this behaviour was changed and conntracks are enabled in host system by default.

Subject: Re: OpenVZ and IP masquerading
Posted by [Santi](#) on Mon, 24 Apr 2006 10:38:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

Thanks for the reply!

Loading "`ip_conntrack`" module with the additional parameter "`ip_conntrack_enable_ve0=1`" NAT works fine with local network machines

I can "ping" the VPS from the hardware node but it's not accesible from the local network, this is the system configuration:

Quote:

ifconfig

```
eth0    Link encap:Ethernet  HWaddr 00:05:1C:19:67:F4
        inet addr:xxx  Bcast:255.255.255.255  Mask:255.255.224.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:4037958 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3702217 errors:0 dropped:0 overruns:7 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2993967675 (2.7 GiB)  TX bytes:1101935960 (1.0 GiB)
        Interrupt:10 Base address:0xdc00

eth1    Link encap:Ethernet  HWaddr 00:05:1C:03:26:36
        inet addr:192.168.0.210  Bcast:192.168.0.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1657862 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2360321 errors:0 dropped:0 overruns:10 carrier:0
```

collisions:0 txqueuelen:1000
RX bytes:285203826 (271.9 MiB) TX bytes:2778409189 (2.5 GiB)
Interrupt:11 Base address:0xe000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:18519 errors:0 dropped:0 overruns:0 frame:0
TX packets:18519 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1587694 (1.5 MiB) TX bytes:1587694 (1.5 MiB)

venet0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
RX packets:16235 errors:0 dropped:0 overruns:0 frame:0
TX packets:23251 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1167074 (1.1 MiB) TX bytes:26626787 (25.3 MiB)

midori:~# route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.0.5	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
xxx 0.0.0.0	255.255.224.0	U	0	0	0	0	eth0
0.0.0.0	xxx 0.0.0.0	UG	0	0	0	0	eth0

eth0 is has the Internet DHCP conection and eth1 is conected to local network...

When starting the VPS with "vzctl" command I get those warnings:

Quote:

midori:/vz/template/cache# vzctl --verbose start 101

Warning: no vz_get_mod_info found in /usr/lib/vz//libvzctl-fs.so

Starting VPS ...

Running: /usr/sbin/vzquota show 101

Running: /usr/sbin/vzquota on 101 -r 0 -b 1048676 -B 1153534 -i 200100 -l 220100 -e 0 -n 0 -s 0

Mounting root: /vz/root/101 /vz/private/101

VPS is mounted

Adding IP address(es): 192.168.0.5

Running: /usr/share/vz/vps-net_add

arp send: can't get iface 'eth0:' address : Cannot assign requested address

vps-net_add WARNING: arp send -c 1 -w 1 -D -e 192.168.0.5 eth0: FAILED

arp send: can't get iface 'eth1:' address : Cannot assign requested address

vps-net_add WARNING: arp send -c 1 -w 1 -D -e 192.168.0.5 eth1: FAILED

```
arp send: can't get iface 'eth0:' address : Cannot assign requested address
vps-net_add WARNING: arp send -c 1 -w 1 -U -i 192.168.0.5 -e 192.168.0.5 eth0: FAILED
arp send: can't get iface 'eth1:' address : Cannot assign requested address
vps-net_add WARNING: arp send -c 1 -w 1 -U -i 192.168.0.5 -e 192.168.0.5 eth1: FAILED
Running VPS script: /usr/share/vz/dists/scripts/debian-add_ip.sh
Setting CPU units: 1000
Set hostname: vps101.usansolo.org
Running VPS script: /usr/share/vz/dists/scripts/debian-set_hostname.sh
Running VPS script: /usr/share/vz/dists/scripts/set_dns.sh
File resolv.conf was modified
Running: /usr/sbin/vzquota stat 101 -f
Running: vzquota setlimit 101 -b 1048576 -B 1153434 -i 200000 -l 220000 -e 0 -n 0
VPS start in progress...
```

Thanks!

--

Santi Saez

Subject: Re: OpenVZ and IP masquerading
Posted by [dev](#) on Mon, 24 Apr 2006 14:20:05 GMT
[View Forum Message](#) <> [Reply to Message](#)

can you provide:
ip a l
ip r l
output please?

Subject: Re: OpenVZ and IP masquerading
Posted by [Santi](#) on Mon, 24 Apr 2006 14:42:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello dev,

Command outputs, "xxx" == public IP address:

Quote:

midori:~# ip a l

```
2: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
```

```
4: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:05:1c:19:67:f4 brd ff:ff:ff:ff:ff:ff
```

```
inet xxx/19 brd 255.255.255.255 scope global eth0
6: eth1: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:05:1c:03:26:36 brd ff:ff:ff:ff:ff:ff
   inet 192.168.0.210/24 brd 192.168.0.255 scope global eth1
3: venet0: <BROADCAST,POINTOPOINT,NOARP,UP> mtu 1500 qdisc noqueue
   link/void
```

```
midori:~# ip r l
192.168.0.5 dev venet0 scope link src xxx
192.168.0.0/24 dev eth1 proto kernel scope link src 192.168.0.210
83.213.128.0/19 dev eth0 proto kernel scope link src xxx
default via 83.213.128.1 dev eth0
```

Regards,

--

Santi Saez
