
Subject: Transparent tcp proxy with haproxy in OpenVZ container

Posted by [grizzly](#) on Thu, 28 Aug 2014 11:10:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello!

Is there any chance to set Transparent tcp proxy in vz container with haproxy?

Tried to set testing environment based on howto from haproxy blog but had no luck

What I did:

1. Enabled all modules for NETFILTER in container and restarted CT:

```
# cat /etc/vz/conf/105.conf | grep NETFILTER
NETFILTER="full"
```

```
HN: # sysctl -a | grep -E 'ip_forward|nonlocal_bind'
net.ipv4.ip_nonlocal_bind = 1
net.ipv4.ip_forward = 1
```

```
CT: # sysctl -a | grep -E 'ip_forward|nonlocal_bind'
net.ipv4.ip_nonlocal_bind = 1
net.ipv4.ip_forward = 1
```

3. Added mangle rules and routes to CT:

```
iptables -t mangle -N DIVERT
iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
iptables -t mangle -A DIVERT -j MARK --set-mark 1
iptables -t mangle -A DIVERT -j ACCEPT
ip rule add fwmark 1 lookup 100
ip route add local 0.0.0.0/0 dev lo table 100
```

```
CT# iptables -t nat -L && iptables -t filter -L && iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source                destination
```

```
Chain POSTROUTING (policy ACCEPT)
target    prot opt source                destination
```

```
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
```

```
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
```

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain PREROUTING (policy ACCEPT)

target prot opt source destination

DIVERT tcp -- anywhere anywhere socket

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

Chain DIVERT (1 references)

target prot opt source destination

MARK all -- anywhere anywhere MARK set 0x1

ACCEPT all -- anywhere anywhere

CT# ip rule list

0: from all lookup local

32765: from all fwmark 0x1 lookup 100

32766: from all lookup main

32767: from all lookup default

4. Build haproxy RPM with TPROXY:

CT# haproxy -vv

HA-Proxy version 1.5.3 2014/07/25

Copyright 2000-2014 Willy Tarreau <w@1wt.eu>

Build options :

TARGET = linux26

CPU = native

CC = gcc

CFLAGS = -m64 -march=x86-64 -O2 -march=native -g -fno-strict-aliasing

OPTIONS = USE_LINUX_TPROXY=1 USE_ZLIB=1 USE_NETFILTER=1 USE_PCRE=1

5. Configured haproxy to catch marked packets

global

log 127.0.0.1 local0

log 127.0.0.1 local1 notice

```
maxconn 4096
daemon
```

defaults

```
log    global
mode   tcp
option tcplog
option dontlognull
retries 3
option redispatch
maxconn 2000
timeout connect 5000
timeout client 50000
timeout server 50000
```

frontend smtp_in

```
bind *:587 transparent
default_backend smtp_out
```

backend smtp_out

```
source 0.0.0.0 usesrc clientip
server mx 10.1.1.102:587 check
```

6. Testing

```
telnet> quit
```

Connection closed.

```
$ telnet <public_ip> 587
```

Trying <public_ip>...

Connected to <public_ip>.

Escape character is '^['.

and nothing happens...

```
CT# tcpdump -i lo
```

shows no activity during telnetting 587 port

When commenting 'source 0.0.0.0 usesrc clientip' all works except that proxy is not transparent

```
$ telnet <public_ip> 587
```

Trying <public_ip>...

Connected to <public_ip>.

Escape character is '^['.

220 mx.domain.com ESMTP

^]

When setting same on HN - transparent proxy works great

```
uname -a
```

Linux domain.com 2.6.32-042stab093.4

```
rpm -qa | grep vz
vzctl-core-4.7.2-1.x86_64
vzquota-3.1-1.x86_64
vzkernel-2.6.32-042stab093.4.x86_64
vzstats-0.5.3-1.noarch
vzctl-4.7.2-1.x86_64
vzdump-1.2-4.noarch
e2fsprogs-resize2fs-static-1.42.11-1.ovz.x86_64
```

```
CT# ip rule list
0: from all lookup local
32765: from all fwmark 0x1 lookup 100
32766: from all lookup main
32767: from all lookup default
```

Will appreciate for help!

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Thu, 28 Aug 2014 12:47:17 GMT
[View Forum Message](#) <> [Reply to Message](#)

Ooops, here is current list of routes from CT

```
CT# ip rule list
0: from all lookup local
32765: from all fwmark 0x1 lookup 100
32766: from all lookup main
32767: from all lookup default
```

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [curx](#) on Thu, 28 Aug 2014 14:13:07 GMT
[View Forum Message](#) <> [Reply to Message](#)

Are the linux kernel tproxy modules loaded on hardware node, plz post the output:

```
lsmod | grep -i tproxy
```

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Thu, 28 Aug 2014 14:21:42 GMT
[View Forum Message](#) <> [Reply to Message](#)

Nope

```
# lsmod | grep -i tproxy
#
```

```
# modprobe tproxy
FATAL: Module tproxy not found.
```

Strange... So it's not compiled in vkernel?

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Fri, 29 Aug 2014 08:29:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

Any advice how to deal with this situation?

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Fri, 29 Aug 2014 08:45:13 GMT
[View Forum Message](#) <> [Reply to Message](#)

But on HN I see that TPROXY compiled as module in kernel:
HN# grep TPROXY /boot/config-2.6.32-042stab093.4
CONFIG_NETFILTER_TPROXY=m
CONFIG_NETFILTER_XT_TARGET_TPROXY=m

Also I checked in default kernel - also got no tproxy with lsmod:
\$ uname -a
Linux domain.com 2.6.32-431.20.5.el6.x86_64
\$ grep TPROXY /boot/config-2.6.32-431.20.5.el6.x86_64
CONFIG_NETFILTER_TPROXY=m
CONFIG_NETFILTER_XT_TARGET_TPROXY=m
\$ lsmod | grep tproxy
\$

So vkernel indeed compiled with needed modules but I still don't get why its not working...

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Fri, 29 Aug 2014 08:59:46 GMT
[View Forum Message](#) <> [Reply to Message](#)

I managed to enable module on HN by enable it with modprobe:

```
HN# lsmod | grep tproxy
nf_tproxy_core      1380  0 [permanent]
```

restarted vz, again added firewall rules and routes, restarted haproxy but still get

```
telnet <public_ip> 587
Trying <public_ip>...
Connected to <public_ip>.
Escape character is '^]'.
and nothing
```

```
tcpdump -i lo
nothing
```

without options 'source 0.0.0.0 usesrc clientip' - works but non transparent

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container
Posted by [grizzly](#) on Fri, 29 Aug 2014 11:29:43 GMT
[View Forum Message](#) <> [Reply to Message](#)

After some testing found that packets are marked well and proxy pass client IP to destination, but outgoing packets goes nowhere

```
# netstat -ctnup | grep 10.1.1.102
tcp      0    1 <client_ip>:39008      10.1.1.102:587        SYN_SENT  696/haproxy
tcp      0    1 <client_ip>:39008      10.1.1.102:587        SYN_SENT  696/haproxy
tcp      0    1 <client_ip>:39008      10.1.1.102:587        SYN_SENT  696/haproxy
tcp      0    1 <client_ip>:39008      10.1.1.102:587        SYN_SENT  696/haproxy
```

In 10.1.1.102 tcpdump shows nothing

Firewall pass all dest ips
-A FORWARD -p tcp -m tcp -d 10.1.1.102/32 --dport 587 -j ACCEPT

But in normal mode

```
netstat -ctnup | grep 10.1.1.102
tcp      0    0 10.1.1.105:58548      10.1.1.102:587        ESTABLISHED 732/haproxy
tcp      0    0 10.1.1.105:58548      10.1.1.102:587        ESTABLISHED 732/haproxy
tcp      0    0 10.1.1.105:58548      10.1.1.102:587        ESTABLISHED 732/haproxy
tcp      0    0 10.1.1.105:58548      10.1.1.102:587        ESTABLISHED 732/haproxy
```

Also tried to proxy to external source and loocked tcpdump on HN - nothing goes to external IP from haproxy in transparent mode

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container

Posted by [grizzly](#) on Fri, 29 Aug 2014 15:03:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

Please help

Subject: Re: Transparent tcp proxy with haproxy in OpenVZ container

Posted by [maykel535](#) on Mon, 25 May 2015 16:06:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hi grizzly, Solved this problem?
