
Subject: How to access internet in container

Posted by [shu7734](#) on Wed, 28 Jan 2015 07:18:59 GMT

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

I try todo Using_NAT_for_container_with_private_IPs from Openvz Wiki page

```
/etc/modprobe.d/openvz.conf
options nf_conntrack ip_conntrack_disable_ve0=0
```

```
/etc/sysctl.conf
net.ipv4.ip_forward = 1
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.all.forwarding=1
```

and reboot

```
iptables -F -t nat
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 61.x.x.x
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 61.x.x.x
iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
iptables -A FORWARD -d 10.0.0.0/24 -j ACCEPT
```

i try

```
vzctl exec 110 ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 61.x.x.x icmp_seq=1 Destination Host Prohibited
From 61.x.x.x icmp_seq=2 Destination Host Prohibited
From 61.x.x.x icmp_seq=3 Destination Host Prohibited
From 61.x.x.x icmp_seq=4 Destination Host Prohibited
^C
```

i find iptables log

```
Jan 28 14:37:55 localhost kernel: [18835.606206] TRACE: raw:OUTPUT:policy:2 IN=
OUT=venet0 SRC=61.x.x.x DST=10.0.0.110 LEN=112 TOS=0x00 PREC=0xC0 TTL=64 ID=1462
PROTO=ICMP TYPE=3 CODE=10 [SRC=10.0.0.110 DST=8.8.8.8 LEN=84 TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=64257 SEQ=3 ]
Jan 28 14:37:55 localhost kernel: [18835.606230] TRACE: mangle:OUTPUT:policy:1 IN=
OUT=venet0 SRC=61.x.x.x DST=10.0.0.110 LEN=112 TOS=0x00 PREC=0xC0 TTL=64 ID=1462
PROTO=ICMP TYPE=3 CODE=10 [SRC=10.0.0.110 DST=8.8.8.8 LEN=84 TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=64257 SEQ=3 ]
Jan 28 14:37:55 localhost kernel: [18835.606241] TRACE: filter:OUTPUT:rule:2 IN= OUT=venet0
SRC=61.x.x.x DST=10.0.0.110 LEN=112 TOS=0x00 PREC=0xC0 TTL=64 ID=1462
PROTO=ICMP TYPE=3 CODE=10 [SRC=10.0.0.110 DST=8.8.8.8 LEN=84 TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=64257 SEQ=3 ]
Jan 28 14:37:55 localhost kernel: [18835.606250] TRACE: mangle:POSTROUTING:policy:1 IN=
```

```
OUT=venet0 SRC=61.191.56.154 DST=10.0.0.110 LEN=112 TOS=0x00 PREC=0xC0 TTL=64
ID=1462 PROTO=ICMP TYPE=3 CODE=10 [SRC=10.0.0.110 DST=8.8.8.8 LEN=84 TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=64257 SEQ=3 ]
```

```
#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
SNAT      all  --  10.0.0.0/24          anywhere        to:61.x.x.x
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target    prot opt source                destination
```

```
Chain INPUT (policy ACCEPT)
```

```
target    prot opt source                destination
ACCEPT    all  --  anywhere             anywhere        state RELATED,ESTABLISHED
ACCEPT    icmp --  anywhere             anywhere
ACCEPT    all  --  anywhere             anywhere
ACCEPT    tcp  --  anywhere             anywhere        state NEW tcp dpt:ssh
ACCEPT    tcp  --  10.0.0.0/24          anywhere        state NEW tcp dpt:mysql
ACCEPT    tcp  --  anywhere             anywhere        state NEW tcp dpt:upnotifyps
ACCEPT    tcp  --  anywhere             anywhere        state NEW tcp dpt:http
ACCEPT    tcp  --  anywhere             anywhere        state NEW tcp dpt:xsync
ACCEPT    tcp  --  anywhere             anywhere        tcp dpts:ndmp:trisoap
REJECT    all  --  anywhere             anywhere        reject-with icmp-host-prohibited
```

```
Chain FORWARD (policy ACCEPT)
```

```
target    prot opt source                destination
REJECT    all  --  anywhere             anywhere        reject-with icmp-host-prohibited
ACCEPT    all  --  10.0.0.0/24          anywhere
ACCEPT    all  --  anywhere             10.0.0.0/24
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target    prot opt source                destination
ACCEPT    tcp  --  anywhere             anywhere        tcp spts:ndmp:trisoap
```

```
Chain PREROUTING (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 POSTROUTING (policy ACCEPT)

target prot opt source destination

all container can't access internet

Subject: Re: How to access internet in container

Posted by [Paparaciz](#) on Mon, 02 Feb 2015 21:11:33 GMT

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

I always like to see iptables-save output. it is more clear for me see whole picture

However I have noticed some strange rule sequence (besides other which I'm not completely sure):

Quote:

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

ACCEPT all -- 10.0.0.0/24 anywhere

ACCEPT all -- anywhere 10.0.0.0/24

so basicaly as first rule you REJECT any forward policy?

Subject: Re: How to access internet in container

Posted by [shu7734](#) on Thu, 05 Feb 2015 01:33:09 GMT

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

because i excute command

```
#iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
```

```
#iptables -A FORWARD -d 10.0.0.0/24 -j ACCEPT
```

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

ACCEPT all -- 10.0.0.0/24 anywhere

ACCEPT all -- anywhere 10.0.0.0/24

the first is default policy

i forget it....

i delete the policy ,
now, is worked!

thanks!
