Subject: Config Iptables macht probleme
Posted by cryordies on Sun, 15 Dec 2013 19:19:47 GMT
View Forum Message <> Reply to Message

Hallo.

Habe ein kleines Problem was iptables angeht.
Ich bekomm das nicht auf die Reihe mit der richtigen Konfiguration.

Habe schon par sachen ausprobiert die aber nicht funktionierten.
iptables ist sehr komplex finde ich und kann schnell verwirrend sein.

Hier mein Vorhaben:

Alle Gast VMs die dem IP-Bereich 10.0.0.1 bis 10.0.0.32 liegen, sollen über den Host vollen Internet Zugang haben.
Eingehende Verbindungen sollen über den entsprechenden Port laufen.
Sprich NAT-Verfahren.

Host ist Debian 7 und Gast ist ebenfalls Debian 7.
Verwenden zu ich das OpenVZ Web Panel 2.4
Vielleicht hat der ein oder andere da par Tipps für mich.

Subject: Re: Config Iptables macht probleme
Posted by curx on Sun, 15 Dec 2013 20:34:34 GMT
View Forum Message <> Reply to Message

Hi,

schau bitte mal is Wiki:
http://wiki.openvz.org/Using_NAT_for_container_with_private_ IPs

Gruß,
Thorsten

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Sun, 15 Dec 2013 20:41:14 GMT
View Forum Message <> Reply to Message

Hallo Thorsten, danke für die schnelle Antwort.
Ich habe mir diesen Artikel im Wiki schon betrachtet, doch leider werd ich da nicht schlau drauß.
Eher gesagt das verwird mich.

Lg

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Sun, 15 Dec 2013 21:58:49 GMT
View Forum Message <> Reply to Message

Wenn ich diese Anleitung befolge bekomm ich von der VM dennoch keine Verbindung. Das anpingen von Host zu Gast und umgekehrt ist möglich.

Hier ein Auszug von ifconfig der VM:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  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:127.0.0.2  P-t-P:127.0.0.2  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:221 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23367 (23.3 KB)  TX bytes:27176 (27.1 KB)

venet0:0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.0.1  P-t-P:192.168.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
```

Vom Host:

```
eth0      Link encap:Ethernet  HWaddr 00:1c:14:01:66:c0
          inet addr:88.198.xxx.xxx  Bcast:88.198.170.135  Mask:255.255.255.248
          inet6 addr: 2a01:4f8:xxx:xxx::2/64 Scope:Global
          inet6 addr: fe80::21c:14ff:xxxx:66c0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:353709 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17852178 (17.0 MiB)  TX bytes:2789605 (2.6 MiB)
```

Interrupt:10 Base address:0xe000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:83809 errors:0 dropped:0 overruns:0 frame:0
TX packets:83809 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:13808384 (13.1 MiB) TX bytes:13808384 (13.1 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:251 errors:0 dropped:0 overruns:0 frame:0
TX packets:273 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:30804 (30.0 KiB) TX bytes:26094 (25.4 KiB)

Subject: Re: Config Iptables macht probleme
Posted by curx on Mon, 16 Dec 2013 11:57:53 GMT
View Forum Message <> Reply to Message

Hi,

zerlegen wir doch mal das Ganze:

*)Alle Gast VMs die dem IP-Bereich 10.0.0.1 bis 10.0.0.32 liegen, sollen über den Host vollen Internet Zugang haben.

- ich nehme mal an das die IP-Range des Internen Netz ein 10.0.0.0/24 ist, es findet kein weiteres Subnetting statt, dann hilft hier ein "Maskieren" via SNAT weiter
- das Netzwerkinferface ins WAN ist die eth0
- die Öffentliche IPv4 Addr des Server liegt in der Range 88.198.170.(129-135) (bitte die richtige auswählen!)
- es sind keine IPTables Regel aktiv

HOSTNODE#> iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 88.198.170.X

*)Eingehende Verbindungen sollen über den entsprechenden Port laufen. Sprich NAT-Verfahren.

- Annahme Hostnode:Port wird auf VM:Port "weitergeleitet" via DNAT, der Port steht der

Hostnode nicht mehr zur Verfügung!
- das Netzwerkinferface ins WAN ist die eth0
- am Beispiel eines Webservers auf Port 80/tcp
- Container IP 10.0.0.2

HOSTNODE#> iptables -t nat -A PREROUTING -p tcp -d 88.198.170.X -dport 80 -i eth0 -j DNAT --to-destination 10.0.0.2:80

Gruß,
Thorsten

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Mon, 16 Dec 2013 16:47:05 GMT
View Forum Message <> Reply to Message

curx wrote on Mon, 16 December 2013 06:57Hi,

zerlegen wir doch mal das Ganze:

*)Alle Gast VMs die dem IP-Bereich 10.0.0.1 bis 10.0.0.32 liegen, sollen über den Host vollen Internet Zugang haben.

- ich nehme mal an das die IP-Range des Internen Netz ein 10.0.0.0/24 ist, es findet kein weiteres Subnetting statt, dann hilft hier ein "Maskieren" via SNAT weiter
- das Netzwerkinferface ins WAN ist die eth0
- die Öffentliche IPv4 Addr des Server liegt in der Range 88.198.170.(129-135) (bitte die richtige auswählen!)
- es sind keine IPTables Regel aktiv

HOSTNODE#> iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 88.198.170.X

*)Eingehende Verbindungen sollen über den entsprechenden Port laufen. Sprich NAT-Verfahren.

- Annahme Hostnode:Port wird auf VM:Port "weitergeleitet" via DNAT, der Port steht der Hostnode nicht mehr zur Verfügung!
- das Netzwerkinferface ins WAN ist die eth0
- am Beispiel eines Webservers auf Port 80/tcp
- Container IP 10.0.0.2

HOSTNODE#> iptables -t nat -A PREROUTING -p tcp -d 88.198.170.X -dport 80 -i eth0 -j DNAT --to-destination 10.0.0.2:80

Gruß,
Thorsten
Hallo.

Das der Port XY dann nicht mehr für den Host verfügbar ist ist mir bekannt.
Habe den Befehl
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth0 -j SNAT --to 88.198.170.X
ausgeführt im Host. Dennoch bekomm ich keine Verbindung von der VM.Die Host-IP habe ich natürlich durch die richtige ersetzt.
ifconfig der VM:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  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:127.0.0.2  P-t-P:127.0.0.2  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13085 (13.0 KB)  TX bytes:14747 (14.7 KB)

venet0:0  Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.0.0.1  P-t-P:10.0.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
```

Beim Ausführen von apt-get update auf der VM:
Kann keine Links posten, da ich keine mind. 10 Poste habe.
Habe es mal auf Pastebin gelegt.
pastebin (Punk) com/cEPpn9ZY

Hier mal ein Auszug von iptables -L vom Host:

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

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

Chain OUTPUT (policy ACCEPT)
target   prot opt source   destination

Und die /etc/sysctl.conf vom Host:

```
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additonal system variables
# See sysctl.conf (5) for information.
#


# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

##############################################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies

# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
```

```
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#
net.ipv4.ip_forward=1
net.ipv4.conf.default.proxy_arp=0
kernel.sysrq=1
net.ipv4.conf.default.send_redirects=1
net.ipv4.conf.all.send_redirects=0

# On Hardware Node we generally need
# packet forwarding enabled and proxy arp disabled
net.ipv4.ip_forward = 1
net.ipv6.conf.default.forwarding = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.default.proxy_arp = 0

# Enables source route verification
net.ipv4.conf.all.rp_filter = 1

# Enables the magic-sysrq key
kernel.sysrq = 1

# We do not want all our interfaces to send redirects
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.all.forwarding=1
```

Lg

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Mon, 16 Dec 2013 17:59:38 GMT
View Forum Message <> Reply to Message

Habe die Sysctl neu gemacht und jetzt funktioniert es. Aber ein Problem ist noch da, die Port DNAT funktioniert nicht

iptables -t nat -A PREROUTING -p tcp -d 88.198.170.xxx -dport 1280 -i eth0 -j DNAT --to-destination 10.0.0.1:1280

Fehlermeldung:

iptables v1.4.14: multiple -d flags not allowed

Subject: Re: Config Iptables macht probleme
Posted by curx on Tue, 17 Dec 2013 07:14:18 GMT
View Forum Message <> Reply to Message

Hi,

die Option dport muss mit zwei Bindestriche begonnnen werden:

iptables -t nat -A PREROUTING -p tcp -d 88.198.170.xxx --dport 1280 -i eth0 -j DNAT --to-destination 10.0.0.1:1280

Wurde bei dem Beispiel vergessen

Kannst Du bitte noch schreiben, was du wegen deinem sysctl Problem gemacht hast?

Gruß,
Thorsten

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Tue, 17 Dec 2013 08:17:37 GMT
View Forum Message <> Reply to Message

Ich habe die neu erstellt und dann die zwei Einträge aus dem Wiki eingesetzt. Und mit sysctl -p aktualisiert. Dann funktionierte es. Die war wohl verpfucht durch verschiedene Versuche. Vielen Dank für deine Hilfe

Subject: Re: Config Iptables macht probleme
Posted by cryordies on Fri, 20 Dec 2013 21:00:01 GMT
View Forum Message <> Reply to Message

Hallo.

Vorab, ich wollte jetzt nicht umbedingt ein neues Thema aufmachen. Hoffe das ist okay.

Zum eigendlichen Problem:

1)
Beim Erstellen eines VPS habe ich eine Differenz (sag ich jetzt mal).
In der Server-Vorlage sind 110GB Diskspace eingestellt, auf der VM habe mit df -h:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/simfs       65G  779M   61G   2% /
none            256M  4.0K  256M   1% /dev
none             52M  1.0M   51M   2% /run
none            5.0M     0  5.0M   0% /run/lock
none            256M     0  256M   0% /run/shm
```

Meine eigendliche Root-Partition auf dem Host ist 70GB groß.

Daher meine Vermutung, die virtuellen Festplatten werden auf dem Host im Root Bereich gespeichert.

Gibt es eine möglichkeit das ganze auf meine /home zulegen? Da die am größten ist.

2)

In der Server Vorlage unter Weitere Einstellungen sind alle Werte (Soft und Hard) auf unbegrenzt gestellt. Von vornerein schon so. Ist aber nicht wirklich sinnvoll, da er den Vorgaben aus der Server Vorlage nicht überschreiten soll.

Lg

Subject: Re: Config Iptables macht probleme
Posted by grep on Fri, 10 Jan 2014 01:19:28 GMT
View Forum Message <> Reply to Message

Quote:
Gibt es eine möglichkeit das ganze auf meine /home zulegen? Da die am größten ist.
Schau in /etc/vz/conf/$veid.conf
Dort kannst du den Pfad anpassen. Nach Änderung einfach bereits vorhandenen Daten in den neuen Pfad kopieren.
VE_ROOT und VE_PRIVATE müssen angepasst werden.
Beispiel:
VE_ROOT="/home/root/$VEID"
VE_PRIVATE="/home/private/$VEID"

Zu 2.
Du kannst die Einstellungen ja jederzeit ändern. Außerdem kannst du eigene Templates erstellen und neue Container mit diesem Template erstellen. Es sollten bereits einige vorkonfigurierte Templates in /etc/vz/conf sein (ve-vswap-4g.conf-sample, ve-light.conf-sample, etc.).