Subject: OpenVZ und IPtables
Posted by alfonsodiecko on Tue, 21 Oct 2008 17:30:31 GMT
View Forum Message <> Reply to Message

Hallo,

nach langen rum probieren habe ich mein ersten Container am laufen, nun möchte ich diesen auch über das Inet erreichen. Da ich mir keine zusätzliche IP kaufen möchte, wollte ich das ganze über NAT regeln. Meine öffentliche IP ist „217.172.182.14“ die auf das root System zeigt, der Container hat beim creat die IP 192.168.172.50 erhalten nun möchte ich gerne über SSH von zu Hause auf die VM 101 zugreifen können. Ich habe mein IPTABLES Script um ein paar Zeilen erweitert bin bis jetzt aber nicht zum Ziel gekommen. Die hinzugefügten Zeilen sehen so aus

iptables -A INPUT -p tcp --dport 10122 -j AKZEPTIEREN
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -A PREROUTING -d 217.172.182.14 -i eth0 -p tcp --dport 10122 -j DNAT --to-destination 192.168.172.50:22

Beim Verbinden über ssh kommt aber keine Verbindung zustande, muss man nach der Standard Installation (wie bei http://www.howtoforge.de/howto/installation-und-gebrauch-von-openvz-auf-debian-etch/ an die ich mich gehalten habe) noch einige Schritte ergänzen?

Wäre für weiterführende Infos sehr erfreut und noch mal danke für den schon erbrachten Support!

mfg alfonso

Subject: Re: OpenVZ und IPtables
Posted by curx on Wed, 22 Oct 2008 17:29:02 GMT
View Forum Message <> Reply to Message

Hi,

ohne Deine ganzen IPTables Regeln zu kennen, den TCP Paketen fehlt die (Rück-)Verbindung ins Netz, weiterhin checke bitte wie die FORWARD Policy und FORWARD Regeln eingerichtet sind.

-> http://wiki.openvz.org/Using_NAT_for_container_with_private_ IPs

iptables -t nat -P PREROUTING ACCEPT
iptables -A INPUT -p tcp --dport 10122 -j ACCEPT
...
iptables -t nat -A PREROUTING -d 217.172.182.14 -i eth0 -p tcp --dport 10122 -j DNAT --to-destination 192.168.172.50:22
...
iptables -t nat -A POSTROUTING -s 192.168.172.50/32 -o eth0 -j SNAT --to 217.172.182.14

Wenn du weiteren Container aus dem (Sub-)Netz 192.168.172.0/24 (gehe mal von einem Class C Netz aus) den Zugriff auf den Inet erlauben willst dann wechsle die Source -s gegen das Netz aus.

Gruß,
Thorsten

Subject: Re: OpenVZ und IPtables
Posted by alfonsodiecko on Wed, 22 Oct 2008 19:03:24 GMT
View Forum Message <> Reply to Message

Ich poste am besten mal meinen vollständigen Script
[I]root@salle:/home/christoph$ grep ip /etc/init.d/firewall[/I]
```
echo "iptables werden geladen..."
modprobe ip_conntrack_ftp
modprobe ipt_MASQUERADE
iptables -F
iptables -X
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -N VERWERFEN
iptables -N AKZEPTIEREN
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT  -m state --state INVALID -j VERWERFEN
iptables -A OUTPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A VERWERFEN -j LOG --log-prefix "F_VERWEIGERT:"
iptables -A VERWERFEN -j DROP
iptables -A AKZEPTIEREN -j LOG --log-prefix "F_ERLAUBT:"
iptables -A AKZEPTIEREN -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j AKZEPTIEREN
iptables -A INPUT -p icmp -j AKZEPTIEREN
iptables -A OUTPUT -p icmp -j AKZEPTIEREN
iptables -A INPUT -p udp --dport 53 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 53 -j AKZEPTIEREN
iptables -A OUTPUT -p udp --dport 53 -j AKZEPTIEREN
iptables -A OUTPUT -p tcp --dport 53 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 80 -j AKZEPTIEREN
iptables -A OUTPUT -p tcp --dport 80 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 25 -j AKZEPTIEREN
iptables -A OUTPUT -p tcp --dport 25 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 110 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 143 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 21 -j AKZEPTIEREN
```

iptables -A OUTPUT -p tcp --dport 21 -j AKZEPTIEREN
iptables -A INPUT -p udp --dport 8767 -j AKZEPTIEREN
#iptables -A INPUT -p tcp --dport 14534 -j AKZEPTIEREN
#iptables -A OUTPUT -p tcp --dport 14534 -j AKZEPTIEREN
iptables -A INPUT -p tcp --dport 10000 -j AKZEPTIEREN
iptables -t nat -P PREROUTING ACCEPT
iptables -A INPUT -p tcp --dport 10122 -j AKZEPTIEREN
iptables -t nat -A PREROUTING -d 217.172.182.14 -i eth0 -p tcp --dport 10122 -j DNAT
--to-destination 192.168.172.50:22
iptables -t nat -A POSTROUTING -s 192.168.172.50/32 -o eth0 -j SNAT --to 217.172.182.14
echo "iptables sind geladen"

Die Konfiguration für forward wurde nach
http://wiki.openvz.org/Using_NAT_for_container_with_private_ IPs übernommen. Liegt es an den IPtables ?

Subject: Re: OpenVZ und IPtables
Posted by alfonsodiecko on Mon, 17 Nov 2008 10:07:25 GMT
View Forum Message <> Reply to Message

Könnt ihr mal euren eigenen IPtables Script posten, wo es funktioniert ?

Subject: Re: OpenVZ und IPtables
Posted by alfonsodiecko on Thu, 20 Nov 2008 14:30:43 GMT
View Forum Message <> Reply to Message

Müsste ich noch diesen schritt hinzufügen ? Oder macht das openVZ alleine ?

Wenn ich modprobe ip_conntrack ip_conntrack_enable_ve0=1
eingebe kommt "WARNING: /etc/modprobe.conf line 1: ignoring bad line starting with 'modprobe'".

Subject: Re: OpenVZ und IPtables
Posted by curx on Mon, 29 Dec 2008 20:47:03 GMT
View Forum Message <> Reply to Message

Die "DEFAULT" FORWARD POLICY wurde auf DROP gestellt;
-> die IP Pakete zwischen der Netzwerkkarte eth0 und
den "virtuellen" Netzdevice venet0 werden geblockt.

[...]
/sbin/iptables -A FORWARD -i eth0 -o venet0 -j ACCEPT
/sbin/iptables -A FORWARD -o eth0 -i venet0 -j ACCEPT

/sbin/iptables -A FORWARD -i venet0 -o venet0 -j ACCEPT
[...]

Subject: Re: OpenVZ und IPtables
Posted by alfonsodiecko on Wed, 31 Dec 2008 11:38:38 GMT
View Forum Message <> Reply to Message

Ok danke jetzt funktioniert schon einmal mein ssh. Habe nun ein weiteres Problem, "apt-get install" funktioniert nicht, es kommt zu Fehlermeldungen wie "Err http://download.openvz.org etch Release.gpg Temporary failure resolving 'download.openvz.org'".

Welche zusätzlichen Schritte muss ich nun beachten ?

Subject: Re: OpenVZ und IPtables
Posted by curx on Wed, 31 Dec 2008 12:26:23 GMT
View Forum Message <> Reply to Message

die DNS Auflösung im Container funktioniert, daher prüfe bitte ob:

- die resolv.conf gültige IP Werte eingetragen hat
- die DNS Anfragen nicht per IPtables geblockt werden

Gruß,
Thorsten