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
