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 ?
