Subject: Problem mit IPtables innerhalb VE 64bit <-> 32bit
Posted by Tobi2WO on Tue, 21 Jul 2009 07:51:32 GMT
View Forum Message <> Reply to Message

Folgende Konstellation: Ich habe eine 32Bit Debian Lenny VE. Dort läuft ein Webserver. Es gibt eine Iptables OUTPUT Regel innerhalb dieser VE, um ausgehenden Traffic für einen bestimmten TCP Port an meine Public IP zu einer anderen VE (10.0.0.106) umzuleiten. Dies hat auf meinem alten 32Bit Rootserver einwandfrei funktioniert. Jetzt bin ich umgestiegen auf Debian Lenny 64 Bit. Alle VEs laufen weiter auf 32Bit.
Alles einwandfrei, nur die OUTPUT Regel funktioniert nur dann für ein paar Minuten, wenn man kurz 10.0.0.106 per Hand mit Telnet kontaktiert (aus der VE). Nach einer kurzen Zeit scheint er die Regel vergessen zu haben und der Port wird nicht weiter umgeleitet.

Einziger Unterschied (neben Umstieg auf 64 Bit) ist, dass ich den Standard OpenVZ Kernel von Debian nutze (2.6.26). Vorher war es ein selbst gestrickter Vanilla 2.6.18 mit OpenVZ Patch.

Bitte um Hilfe

Subject: Re: Problem mit IPtables innerhalb VE 64bit <-> 32bit
Posted by curx on Tue, 21 Jul 2009 11:48:03 GMT
View Forum Message <> Reply to Message

Hi,

was sagen die conntrack tabellen des Containers :

# cat /proc/net/ip_conntrack

Subject: Re: Problem mit IPtables innerhalb VE 64bit <-> 32bit
Posted by Tobi2WO on Tue, 21 Jul 2009 13:21:25 GMT
View Forum Message <> Reply to Message

Konkret geht es um einen Teamspeak Viewer, der Teamspeak Server läuft auf einer anderen VE (10.0.0.106).

1) telnet *public_ip* 51234
- keine Reaktion
2) grep 51234 /proc/net/ip_conntrack
- keine Ausgabe

3) telnet 10.0.0.106 51234
- Verbindung erfolgreich
4) grep 51234 /proc/net/ip_conntrack

- tcp 6 118 TIME_WAIT src=10.0.0.103 dst=10.0.0.106 sport=54398 dport=51234 packets=5 bytes=274 src=10.0.0.106 dst=10.0.0.103 sport=51234 dport=54398 packets=5 bytes=274 [ASSURED] mark=0 secmark=0 use=1

5) telnet *public_ip* 51234
- diesmal plötzlich erfolgreich
6) grep 51234 /proc/net/ip_conntrack
- zusätzlich zur Ausgabe von oben nun dieser Eintrag:
tcp 6 118 TIME_WAIT src=10.0.0.103 dst=*public_ip* sport=40356 dport=51234 packets=5 bytes=274 src=10.0.0.106 dst=10.0.0.103 sport=51234 dport=40356 packets=5 bytes=274 [ASSURED] mark=0 secmark=0 use=1

Die Iptables Regel ist:
iptables -t nat -A OUTPUT -d *public_ip*/32 -p tcp -m tcp --dport 51234 -j DNAT --to-destination 10.0.0.106:51234

---

Subject: Re: Problem mit IPtables innerhalb VE 64bit <-> 32bit
Posted by Tobi2WO on Wed, 22 Jul 2009 13:58:44 GMT
View Forum Message <> Reply to Message

Weitere Tests haben ergeben, dass das Problem auch innerhalb einer 64Bit VE besteht.
Werde das mal im englischen Bereich posten.

---