Subject: IPv6 - Route festlegen
Posted by Sven on Mon, 11 May 2009 17:14:46 GMT
View Forum Message <> Reply to Message

Hi there!

Ich hätt' da gern mal ein Problem

Das Grundproblem ist, dass keine IPv6-Routen beim hochfahren der einzelnen Container gesetzt werden, zumindest nicht bei mir.
Ich definiere die statische IPv6-Adresse in der config des containers, die Adresse wird auch zugeteilt, aber es werden keinerlei routen gesetzt.

Aktuell umgehe ich das Problem, indem ich auf dem Hostsystem nach dem hochfahren folgendes kleines script starte:

```
#! /bin/bash

for i in `seq 101 114`; do
        echo "Lege IPv6-Route in $i an..."
        /usr/sbin/vzctl exec $i /sbin/ip -6 route add ::/0 dev venet0
done
```

Finde das nur ein wenig unelegant, habe aber keine Möglichkeit gefunden, das Script sinnvoll in dem container starten zu lassen, da die IPv6-Adresse recht spät zugewiesen wird, und ich das somit nicht über das initsystem machen kann.
Gibts keine Möglichkeit die routen im Startvorgang der container anlegen zu können?

Dann habe ich das Problem, dass die conntrack-engine für die VPS ein wenig strubbelig zu sein scheint.
Zum grundsätzlichen Aufbau des Rulesets:
Ich werfe alles anhand des Eingans-Interfaces in verschiedene Chains und filtere dort weiter.
Pakete im Zustand RELATED und ESTABLISHED erlaube ich sehr früh (quasi als erstes, davor habe ich nur eine Chain um den Traffic zu zählen).

Die relevanten Teile meines ip6table-scriptes einmal:

```
# Accounting
$IPT -N ACCOUNTING
$IPT -A INPUT -j ACCOUNTING
$IPT -A OUTPUT -j ACCOUNTING
$IPT -A FORWARD -j ACCOUNTING

# aufgebaute erlauben
$IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

[...]

# Chains fuer die einzelnen If
$IPT -N REDIN
$IPT -A INPUT -i $RED -j REDIN
```

$IPT -A FORWARD -i $RED -j REDIN

[...]

$IPT -N VPSIN
$IPT -A INPUT -i $VPS -j VPSIN
$IPT -A FORWARD -i $VPS -j VPSIN

Zur weiteren Verdeutlichung:
ip6tables -vnxL FORWARD
Chain FORWARD (policy DROP 21 packets, 22255 bytes)
    pkts   bytes target   prot opt in   out   source   destination
 4691726 3882606596 ACCOUNTING all   *   *   ::/0   ::/0
 4655337 3879276130 ACCEPT   all   *   *   ::/0   ::/0   state
RELATED,ESTABLISHED

[...]

   32764 3046910 VPSIN   all   venet0 *   ::/0   ::/0

Das Problem ist nun folgendes:
ip6tables erlaubt auf dem WAN-If ($RED) die Pakete im Zustand RELATED,ESTABLISHED.
Problem ist - der Zustand ist auf dem Eingang des If venet0 scheinbar wieder unbekannt und wird dort verworfen. Der Kernel scheint diese als völlig neue Pakete zu behandeln (im Log werden diese als Eingangs- und Ausgangsinterface venet0 gelogt) - ich muss in der Chain für das If venet0 also auch alle Pakete mit der source-ip !$EIGENES_NETZ erlauben. Auch wenn ich in der Chain für venet0 nochmals alle Pakete im Zustand RELATED oder ESTABLISHED erlaube matchen diese nicht darauf; für die conntrack-engine sind es zu diesem Zeitpunkt Pakete im Zustand NEW, auch wenn die in den vorherigen Chains (Eingang auf dem WAN-If) richtig zugeordnet wurden.

Falls von Interesse:
Auf dem Hostsystem läuft der amd64 Debiankernel (2.6.26-2-openvz-amd64 #1 SMP Fri Mar 27 05:10:50 UTC 2009 x86_64 GNU/Linux), alle Gastsysteme sind Debian-lenny Systeme.
Keine Backports oder sonstige Fremdpakete installiert.

Das System selbst ist allerdings schon ein bissel älter (damals aufgesetzt unter woody und linux-vserver, dann "irgendwann" mal zu openvz migriert, da lief aber schon etch), falls das von Interesse sein sollte.