Subject: route vs iptables
Posted by Detlef on Mon, 28 Jul 2014 15:22:23 GMT
View Forum Message <> Reply to Message

Es geht hier um massenhafte Abfilterung von blackgelisteten IPs in mehreren Containern:

iptables - Rules sind durch numiptent in den Containern begrenzt. Sie benötigen Kernel-Speicher und daher soll lt. Doku möglichst wenige numiptent als Max-Werte gesetzt werden. Was verbraucht eine iptables-Regel an Resourcen?

Mit route dagegen, lassen sich viele Wegrouting-Regeln erstellen. Benötigen diese aber keinen Kernel-Speicher? Was verbraucht hier eine route-Regel an Resourcen?

Wenn wir jetzt mal 20000 IPs betrachten, die wir blocken wollen und dies auch noch auf verschiedenen Containern, wie wirken sich die Verwendungen von iptables vs route im Host aus? Was ist schneller, was verbraucht mehr Resourcen?

Wenn wir davon ausgehen, daß wir route verwenden, so können diese auch im Host für alle Container setzen, aber dann wären die Kunden-Container ggf. alle von diesen blackgelisteten IPs gesperrt. Würde dies schneller ablaufen? Würde dies weniger Resourcen verbrauchen? und unter Umständen, greifen diese Routings gar nicht, weil diese z.B. in Verbindung mit MAC dennoch durch geroutet werden.

Warum ich dies jetzt erfrage, hat auch einen entscheidenden Hintergrund, denn routing hat sich zum Blocking vs iptables vorher bei uns ganz gut durch gesetzt und funktionierte einwandfrei. Plesk 12.x bringt nun aber fail2ban mit und hier wird die IP-Filterung wieder nur auf iptables angeboten! Die Frage stellt sich also, warum verwenden die iptables statt route?

Ich freue mich dann auf interessante Ausführungen - Liebe Grüße

Detlef