

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6
für Linux-Server und -Netzwerke



 ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam



28 nf-HiPAC

Sobald Sie mehrere tausend Regeln in einer Kette in Ihrer Firewall verwenden müssen, werden Sie feststellen, dass die Geschwindigkeit der Paketverarbeitung stark sinkt. Dann sollten Sie sich nf-HiPAC (<http://www.hipac.org>) genauer ansehen. Dabei handelt es sich um einen Patch, der mit dem HiPAC-Paketklassifizierungsalgorithmus bei mehr als 1000 Regeln immer noch schneller arbeitet als Iptables mit 100 Regeln. nf-HiPAC unterstützt aktuell fast alle Iptables-Funktionen. Nur NAT wird (noch) nicht unterstützt.

28.1 Was ist nf-HiPAC?

nf-HiPAC ist ein kompletter Paketfilter für Linux, der mit HiPAC einen neuen Algorithmus für die Klassifizierung von Paketen verwendet. Dieser Algorithmus reduziert die Speicherzugriffe je Paket enorm und erreicht so hohe Verarbeitungsgeschwindigkeiten auch bei großen Regelsätzen und Netzen mit großer Auslastung.

nf-HiPAC stellt die gleichen Funktionen wie Iptables zur Verfügung. Die Konfiguration des Paketfilters erfolgt mit dem Werkzeug `nf-hipac`, das in weiten Teilen kompatibel zum Iptables-Befehl ist. Dadurch können viele Skripten durch einen einfachen Austausch des Befehls auf nf-HiPAC umgestellt werden.

Achtung



nf-HiPAC ist ein reiner Paketfilter. NAT oder Mangling werden nicht unterstützt.

Im Gegensatz zu Iptables ist die Geschwindigkeit von nf-HiPAC in fast allen Umgebungen unabhängig von der Größe des Regelsatzes besser. Dieser Unterschied fällt besonders bei großen Regelsätzen auf. Während die Geschwindigkeit von Iptables linear mit der Zahl der Regeln abnimmt, bleibt die von nf-HiPAC nahezu konstant.

Ein Regel-Update führt bei nf-HiPAC nicht zu Verzögerungen in der Bearbeitung. Dynamische Regelsätze können sehr schnell umgesetzt werden. Einzelne Regeln

können entfernt oder ausgetauscht werden, ohne dass es wie bei Iptables zu Verzögerungen kommt.

Da es sich bei nf-HiPAC noch um ein Werkzeug handelt, das sich im Moment in starker Weiterentwicklung befindet und sicherlich nur für einen ganz kleinen Bereich der Leser interessant ist, verweise ich für weitere Informationen auf die Homepage <http://www.hipac.org>.

Hinweis



Eine letzte Bemerkung noch zu nf-HiPAC: Es gibt im Netfilter-Team Überlegungen, nf-HiPAC in das Iptables-Projekt aufzunehmen. Dann ist ein Patchen überflüssig.