nftables – der neue Paketfilter im Linux-Kernel

Dieser Vortrag richtet sich an all diejenigen, die sich für die Zukunft der Paketfilterung unter Linux interessieren. Kenntnisse der Linux-Systemadministration und der aktuellen Paketfilter wären von Vorteil.

nftables, das neue Filtersystem im Linux-Kernel wurde von Grund auf neu entwickelt. Mit der Version 3.13 wurde der Programmquelltext in den Hauptzweig des Linux-Kernels aufgenommen. Obwohl noch in der Entwicklung befindlich, wird es auf lange Sicht gesehen das *iptables*-Framework ablösen. Ziele der Neuentwicklung sind einfachere Wartbarkeit des Quelltextes und eine Beschleunigung der Paketfilterung.

Als Vorbild für *nftables* kann das Berkeley-Paketfiltersystem gesehen werden; beide sind ähnlich konzipiert. Die Architektur ist im Gegensatz zu *iptables* und seinen Verwandten protokollunabhängig. Dadurch existieren keine mehrfach vorhandenen Programmstücke, die die gleiche Filterarbeit verrichten. Im Vortrag wird erklärt, wie *nftables* im Linux-Kernel arbeitet und wie das Regelwerk aus der Administrationsebene im Betriebssystem ankommt. Der Einsatz und die Funktion der genutzten Bibliotheken werden im Zusammenhang erklärt. Das Regelwerk wird bereits im Userspace als Binärprogrammstück in Form einer virtuellen Maschine erstellt und kann vom Kernel verarbeitet werden. Vorteil hierbei ist, dass der Kernel nicht erweitert werden muss, wenn neue Protokollfiltermechanismen hinzugefügt werden. Das Hinzufügen, Löschen und Manipulieren von Regeln ist mit *nftables* einfacher und schneller zu erledigen als mit *iptables*. Neue, von *nftables* unterstützte Funktionen sind das Filtern basierend auf IP-Adressen-Sets oder Mapping-Mechanismen.

Die Handhabung für den Administrator durch das Programm *nft* hat sich im Vergleich zum Aufrufwerkzeug *iptables* ebenfalls verändert. So lässt sich *nft* als Interpreter für Skripte verwenden und die Filteregeln stellen die Skriptsprache dar. Damit die Migration von *iptables* zu *nftables* einfach vonstatten geht, wurde vom Netfilter-Team eigens ein Programm dafür entwickelt. Ebenso wurden einige Verbindungen zum ursprünglichen *xtables*-Framework geschaffen.

Der Vortrag umfasst im Praxisteil die Umwandlung eines vorhandenen *iptables*-Regelwerks nach *nftables* und zeigt Anwendungsfälle von nftables für die typische IT-Landschaft auf.

Weiterführende Links zum Thema:

- Projekt-Homepage: `http://netfilter.org/projects/nftables/`
- Artikel zum Thema *nftables* in den *Linux Weekly News*: `https://lwn.net/Articles/324989/` und `http://lwn.net/Articles/564095/`
- Technische Details: `people.netfilter.org/kaber/nfws2008/nftables.odp`