TECHNISCHE UNIVERSITÄT DRESDEN
Fakultät Informatik Institut für Technische Informatik, Professur für Rechnerarchitektur

iptables und nftables

ein neues Paketfiltersysstem für den Linux Kernel

Präsentation der Abschlussaufgabe im Rahmen des Praktikums
»Linux Cluster in Theorie und Praxis«

von Alfred Krohmer (Gruppe 4, Matrikel 3755190)

Dresden, 28. Feb 2014

DRESDEN concept
Exzellenz aus Wissenschaft und Kultur

Gliederung

1 Einführung

Zielstellungen bei der Entwicklung bei `nftables`

- Vereinfachung der Kernel-ABI
- Vermeidung von Code-Redundanz
- effizientere Abarbeitung der Regeln
- bessere Fehlermeldungen

2 Rückblick / bisherige Firewall-Lösungen

- 1994: ipfw
- 1996: ipfwadm
- 1999: ipchains
- 2000: iptables
- **2014: nftables**

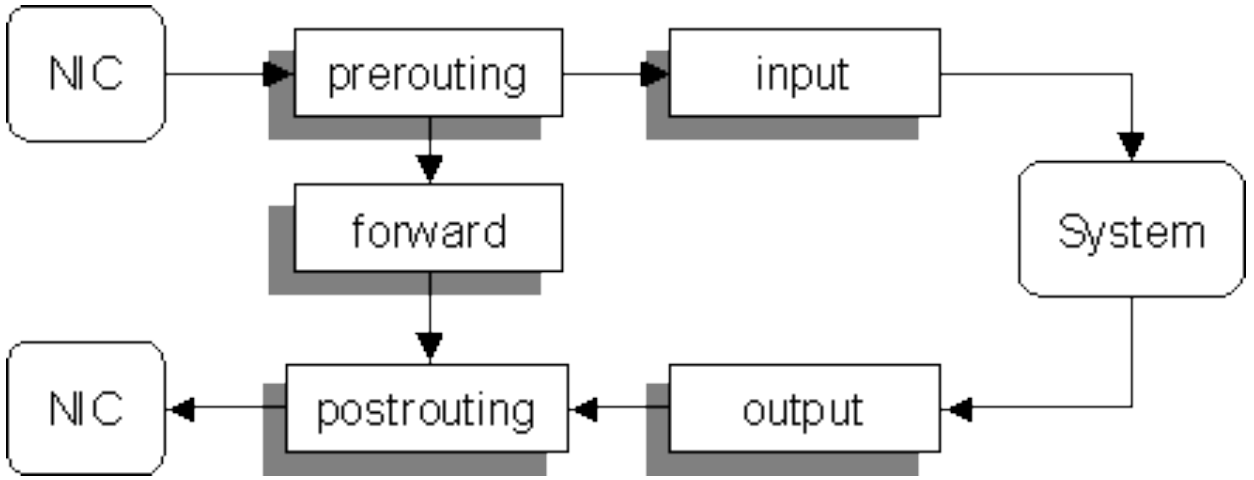
3 Funktionsweise iptables vs. nftables

iptables:

- nur für IPv4
- andere Tools für andere Programme:
  - ip6tables
  - arptables
  - ebtables

3 Funktionsweise iptables vs. nftables

iptables:



http://content.hccfl.edu/pollock/AUnixSec/IptablesOverview_files/image001.gif

3 Funktionsweise iptables vs. nftables

iptables:

- für jedes Protokoll eine eigenständige Implementierung im Kernel
- Code für jedes Protokoll sehr spezifisch
  - viel replizierter Code
  - hohe Performance

3 Funktionsweise iptables vs. nftables

nftables:

- ein Tool für alle Protokolle
  (IPv4, IPv6, Ethernet-Bridging, ARP)
- einheitliche Schnittstelle zum Kernel

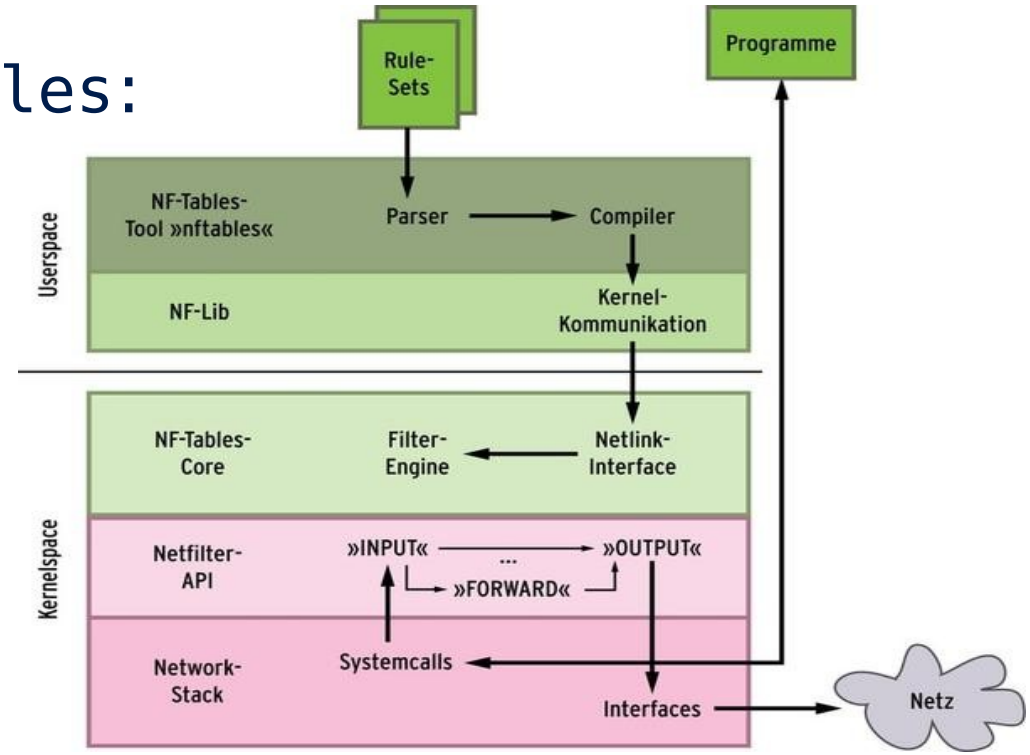
3 Funktionsweise iptables vs. nftables

nftables:

- Implementierung als kleine virtuelle Maschine im Kernel
- Regeln werden im Userspace zu Byte-Code kompiliert

3 Funktionsweise iptables vs. nftables

nftables:



http://www.linux-magazin.de/var/linux_magazin/storage/images/media/linux-magazin/ausgabe/2009/09/wiedergeborener-waechter/abb2.jpg/391614-1-ger-DE/abb2.jpg_reference.jpg

3 Funktionsweise iptables vs. nftables

nftables:

- Byte-Code kann auf Feldern und Bits der Pakete Operationen ausführen:
  - vergleichen (matching) → bedingte Sprünge
  - arithmetische und logische Operationen
  - beliebige Änderungen am Paketinhalt

3 Funktionsweise iptables vs. nftables

nftables:

- payload load 4 offset network header + 16 => reg 1
  compare reg 1 192.168.0.1

- payload load 4 offset network header + 16 => reg 1
  set lookup reg 1 load result in verdict register
  { "192.168.0.1" : jump chain1,
  "192.168.0.2" : drop,
  "192.168.0.3" : jump chain2 }

3 Funktionsweise iptables vs. nftables

nftables:

- atomares Ersetzen von Regeln über Netlink-Transaktionen
- funktioniert mit bisher verfügbaren Tools noch nicht effektiv

4 Syntax / Tools

iptables:

- `iptables -A INPUT -p tcp --dport 22 -j LOG`
- `iptables -A INPUT -p tcp --dport 22 -j DROP`

4 Syntax / Tools

nftables: **nft**

- `nft add table filter`
- `nft add chain filter input \`
  `„{ type filter hook input priority 0; }”`

- `nft add rule filter input \`
  `tcp dport 22 log drop`

nftables: **nft**

- als Script:

```
#!/usr/bin/nft -f
table filter {
  chain input {
    type filter hook input priority 0;
    ip protocol tcp dport 22 drop log
  }
```

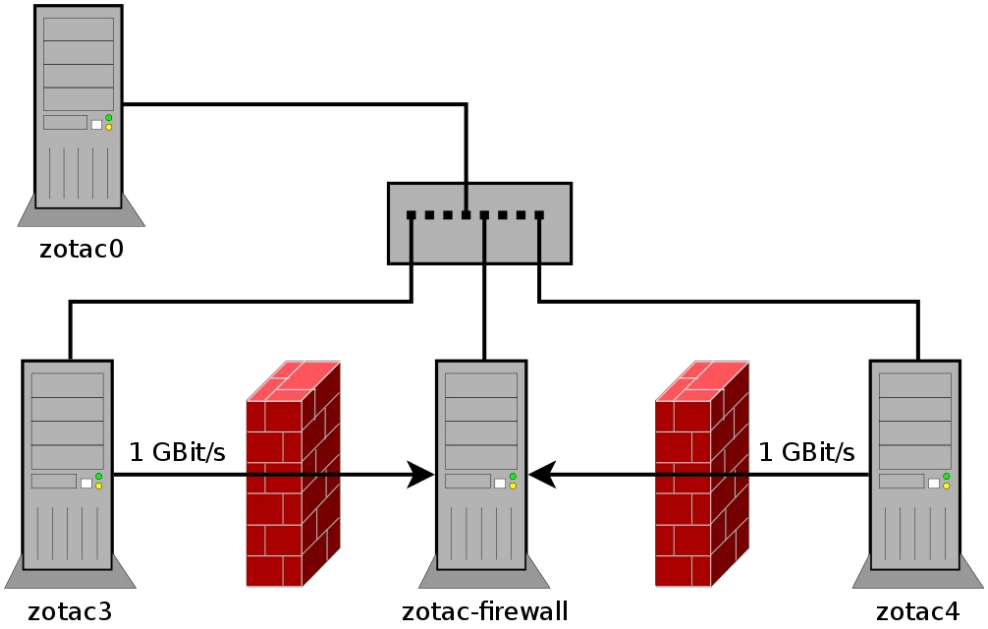
4 Syntax / Tools

`nf`tables: `nft`

- `nft` bisher noch kaum in Linux-Distributionen verfügbar
- in Arch Linux bisher nur im AUR verfügbar

5 Performance-Vergleich

Testaufbau:



Testaufbau

- Hardware:
  - Sender / Empfänger:

    Intel Atom 330 (1,6 GHz), nVidia Chipsatz
  - Firewall: Intel Core 2 Duo E6750 (2,6 GHz)
  - jeweils 2 GB Ram

Testaufbau

- Software:
  - `pktgen`
  - `ifpps` (aus `netsniff-ng`)

Testaufbau

- `zotac3` sendet Pakete über `zotac-firewall` an `zotac4`
- Firewall hat entsprechend viele Regeln
- Empfänger verwirft Pakete noch im `iptables`-Stack

6 Schlussfolgerung

- Performance von `nftables` noch unterlegen
- Optimierungsmöglichkeiten
- Konzept mit virtueller Maschine mächtig
- leichte Erweiterbarkeit
- **bisher allerdings noch nicht im Produktivbetrieb einsatzbereit**

7 Quellen

- Projekt-Website von nftables:
  http://netfilter.org/projects/nftables/
- Tutorial von Eric Leblond:
  https://home.regit.org/netfilter-en/nftables-quick-howto/

7 Quellen

- nftables Wiki:
  `http://wiki.nftables.org/wiki-nftables/index.php/Main_Page`
- Wikipedia-Artikel:
  `http://en.wikipedia.org/wiki/Nftables`

»Wissen schafft Brücken.«