Grundlagen iptables

Damit ein Linuxsystem eine Paketfilterfirewall benutzen kann wird die Schnittstelle „netfilter“ und das Userfontend „iptables“ benötigt.

Mit „iptables“ definiert man die Firewall-Regeln, die dann über „netfilter“ im Kernel aktiviert werden. Iptables ist in vielen Linux Distributionen Standardmässig enthalten. Sind mit Iptables erstellte Filterregeln konfiguriert, werden alle IP Datenpakete geprüft (ankommende, bevor sie an die Zielanwendung weitergeleitet werden und ausgehende bevor sie den Rechner verlassen).

Wird das System als Router eingesetzt werden die Pakete wärend der weiterleitung geprüft. Pakete können auch manipuliert werden.

Die Paketprüfung und die Filterregeln sind dreistufig aufgebaut (hierarchisch von oben nach unten):

- Tabellen.
- Ketten (Chains).
- Filterregeln.

Trifft eine definierte Regel in einer Tabelle oder Kette zu, wird eine in der Regel definierte Aktion ausgeführt. Trifft keine Regel zu, wird die in der Tabelle gültige Policy angewandt.

Tabellen

In den Tabellen werden Regeln zu Gruppen nach grungsätzlichen Aufgaben unterteilt. Es gibt vier wichtige Tabellen in der Filterregeln hinterlegt werden können.

Tabelle	**Beschreibung**
filter	Standardtabelle, hier werden alle Filterregeln hinterlegt.
nat	Wird für Adressumsetzung und Port Forwarding verwendet.
mangle	wird zur Paketmanipulation eingesetzt.
raw	definiert Ausnahmen von Connection Tracking.

Ketten (Chains)

Jede Tabelle enthält verschiedene Ketten (Chains), die festlegen wann ein Paket geprüft wird (z.B vor der versendung des Pakets), ob die Regel einzufügen oder zu löschen ist. Es gibt fünf Ketten und nicht jede Kette muss in jeder Tabelle vorkommen.

Kette	**für Tabelle**	**Beschreibung**
INPUT	filter, mangle	Hier sind alle Paketregeln enthalten die für den eigenen lokalen Rechner bestimmt sind.
OUTPUT	filter, mangle, nat, raw	Hier sind alle Regeln enthalten die auf ausgehende Pakete von einem lokalen Prozess angewandt werden.
FORWARD	filter, mangle	Hier werden weiterzuleitende Pakete verarbeitet, die greoutet werden.

Kette	für Tabelle	Beschreibung
PREROUTING	nat, mangle, raw	Wird auf Pakete angewandt, bevor sie geroutet werden.
POSTROUTING	nat, mangle	Wird auf Pakete angewandt, nachdem sie geroutet wurden.

Filterregeln

In den Tabellen und Ketten werden die Filterregeln festgelegt. Der Aufruf erfolgt mit „root“ Rechten.

- `iptables <Option>`
- `iptables -L`

Optionen für Filterregeln

Die Regeln werden Zeilenweise durchlaufen. Trifft eine Regel für ein Paket zu wird die Verarbeitung abgebrochen. Ist es eine Benutzerdefinierte Kette, wird der Durchlauf in der aufgerufenen Kette weitergeleitet, ist die Kette eine eingebaute Standardkette, so gilt als Ziel die Policy.

...

http://kreativgarten.bplaced.net/doku.php?id=iptables

Last update: **2019/05/27 16:13**