Wiki / iptables2

Dieser Artikel wurde für die folgenden Ubuntu-Versionen getestet:

Dieser Artikel ist größtenteils für alle Ubuntu-Versionen gültig.

Ausbaufähige Anleitung

Dieser Anleitung fehlen noch einige Informationen. Wenn Du etwas verbessern kannst, dann editiere den Beitrag, um die Qualität des Wikis noch weiter zu verbessern.

Anmerkung: Dieser Artikel beschreibt die grundsätzliche Funktionalität von iptables. Weitere Beispiele und Details, insbesonders zum Thema NAT (Network Address Translation) können hinzugefügt werden.

Zum Verständnis dieses Artikels sind folgende Seiten hilfreich:

1. **Installation von Programmen**
2. **Bearbeiten von Paketquellen**
3. **Ein Terminal öffnen**

Inhaltsverzeichnis

1. Installation
2. Grundlagen der Paketprüfung
3. Funktionsweise von iptables
4. Weitere Optionen und Möglichkeiten
5. Einsatz von iptables
6. Graphische Benutzeroberfläche
7. Links

Mit Hilfe von **iptables** [http://www.iptables.org/projects/iptables/index.html] wird **Netfilter** [http://www.netfilter.org] , der IP-Paketfilter des **Linuxkernels** [https://wiki.ubuntuusers.de/Kernel] konfiguriert. Paketfilter werden üblicherweise in Routern und Firewalls eingesetzt.

iptables und Netfilter wurden mit dem Linux Kernel 2.4 eingeführt und unverändert in den Kernel 2.6 übernommen.

Installation

iptables ist üblicherweise in der Standardinstallation von Ubuntu enthalten. Ansonsten kann das entsprechende Paket

- **iptables**

Jetzt installieren [apt://iptables] mit **apturl** [https://wiki.ubuntuusers.de/apturl]

```
sudo apt-get install iptables
```

nachinstalliert werden [1].

Hinweis:

Die in diesem Artikel dargestellten Inhalte beziehen sich auf die IPv4-Implementation von iptables. Zu beachten ist, dass Rechner in der Standard-Installation zusätzlich immer auch IPv6 bedient und die entsprechenden Regeln analog auch mit **ip6tables** gepflegt werden müssen. Regeln über iptables (=IPv4) haben keinerlei Auswirkungen, wenn der Rechner über IPv6 angesprochen wird und dementsprechend erweist sich die IPv4-iptables als nicht weiter relevant.

Grundlagen der Paketprüfung

Ist der Paketfilter des Kernel aktiv (d.h. sind mit iptabels erstellte Filterregeln konfiguriert), so werden alle IP-Datenpakete geprüft. Ankommende Pakete werden geprüft, bevor sie an die Zielanwendung geleitet werden, ausgehende Pakete werden geprüft, bevor sie den Rechner verlassen. Agiert der Rechner als Router (z.B. in einem Netzwerk), so werden die Pakete während der Weiterleitung geprüft. Außerdem besteht auch die Möglichkeit der Paketmanipulation. Die Art der Prüfung lässt sich mit Hilfe von iptables sehr detailliert vorgeben.

Funktionsweise von iptables

Die Paketprüfung und die mit iptables zu erstellenden Filterregeln sind dreistufig aufgebaut. Es gibt (hierarchisch von oben nach unten):

- Tabellen
- sogenannte "Chains" (Ketten)
- die eigentliche Filterregeln

Trifft eine in einer Tabelle und Chain definierte Regel zu, so wird die in der Regel hinterlegte **Aktion** ausgeführt. Sollte keine Regel zutreffen (was durchaus nichts ungewöhnliches ist), so wird die in der Tabelle hinterlegte, allgemein gültige **Policy** angewendet.

Tabellen

In den Tabellen werden Filterregeln zu Gruppen zusammengefasst, unterteilt nach der grundsätzlichen Aufgabe. Es gibt vier wichtige Tabellen (=Regelsätze), in der die Filterregeln hinterlegt werden können:

verschiedene Tabellen von iptables

Tabelle	Beschreibung
filter	Dies ist die Standardtabelle. Wie der Name vermuten lässt werden hier alle "reinen" Filterregeln hinterlegt.
nat	Diese Tabelle wird in der Regel für Adressumsetzung (NAT = Network Address Translation) und spezielle Weiterleitungen (Port Forwarding) eingesetzt.
mangle	Diese Tabelle wird in der Regel bei gewünschter Paketmanipulation eingesetzt.
raw	Diese Tabelle wird in der Regel eingesetzt um Ausnahmen vom Connection Tracking zu definieren.

Chains

Jede Tabelle enthält verschiedene Chains. Die Chains legen fest, wann ein Paket geprüft wird (z.B. bevor es versendet wird). Es gibt fünf verschiedene Chains, wobei nicht jede Chain in jeder Tabelle vorkommt.

Chains von iptables		
Chain	**für Tabelle**	**Beschreibung**
INPUT	filter, mangle	Wird auf alle Pakete angewendet, die an einen lokalen Prozess gerichtet sind.
OUTPUT	filter, nat, mangle, raw	Wird auf alle Pakete angewendet, die von einem lokalen Prozess stammen.
FORWARD	filter, mangle	Wird auf alle Pakete angewendet, die geroutet werden.
PREROUTING	nat, mangle, raw	Wird auf alle Pakete angewendet, *bevor* diese geroutet werden.
POSTROUTING	nat, mangle	Wird auf alle Pakete angewendet, *nachdem* diese geroutet wurden.

Definition der Filterregel

In den Tabellen und Chains werden die Filterregelsätze festgelegt. Dies geschieht über einen Aufruf von iptables im Terminal [3], wobei die allgemeine Syntax von iptables wie folgt ist:

```
iptables <Option>
```

Hinweis:

Der Aufruf von iptables erfordert immer **Root-Rechte**.

Dazu kennt iptables eine Vielzahl von Optionen, von den im folgenden einige (primär für die Tabelle

"filter" und die Chains INPUT, OUTPUT und FORWARD) erklärt werden.

Optionen für Filterregeln	
Option	**Beschreibung**
-t Tabelle	Diese Filterregel gilt für die Tabelle "Tabelle".
-I Chain [Position]	Regel wird an Position "Position" der Kette "Chain" eingefügt. Bei Nichtangabe der Position wird die Regel am Anfang der Kette eingefügt.
-A Chain	Regel wird an die Kette "Chain" angehängt.
-D Chain	Regel wird aus der Kette "Chain" gelöscht.
-F Chain	Alle Regeln der Kette "Chain" löschen.
-L Chain	Liste alle Regeln der Kette "Chain" auf.
-p Protokoll	Das Paket wird nur geprüft, wenn es gemäß "IP-Protokoll" ist (z.B. TCP, UDP, ICMP).
-s IP-Adresse	Das Paket wird nur geprüft, wenn es von der definierten IP-Adresse stammt.
-d IP-Adresse	Das Paket wird nur geprüft, wenn es an die definierte IP-Adresse gesendet wird.
-i Netzwerkschnittstelle	Das Paket wird nur geprüft, wenn es über die definierte Netzwerkschnittstelle eingegangen ist.
-o Netzwerkschnittstelle	Das Paket wird nur geprüft, wenn es über die definierte Netzwerkschnittstelle versendet wird.
--sport Port-Nr oder --source-port Port-Nr	Das Paket wird nur geprüft, wenn es von der definierten Port-Nummer stammt. Muss zwingend in Verbindung mit -p benutzt werden!
--dport Port-Nr oder -destination-port Port-Nr	Das Paket wird nur geprüft, wenn es an die definierte Port-Nummer gesendet wird. Muss zwingend in Verbindung mit -p benutzt werden!
-j Aktion	Legt fest, welche Aktion auf das Paket angewendet werden soll, wenn alle Prüfkriterien erfüllt wurden. Weitere Details siehe **hier**.
-P Chain Aktion	Legt eine Policy für eine Chain fest, falls keine Filterregel zutrifft. Weitere Details siehe **hier**.

Trifft ein Filterregel auf ein Paket zu, muss noch festgelegt werden, wie mit dem Paket verfahren werden soll (Option -j Aktion, siehe oben). Bei "normaler" Filterung sind die häufigsten Aktionen:

verschiedene Aktionen, die auf ein Paket angewendet werden	
Aktion	**Beschreibung**
ACCEPT	Das Paket wird akzeptiert und angenommen.
DROP	Das Paket wird nicht angenommen, der Sender erhält keine Nachricht.
REJECT	Das Paket wird nicht angenommen, der Sender wird benachrichtigt.
LOG	Die Paketdaten werden im System-Log festgehalten, anschließend wird die nächste Regel der Chain geprüft und ggf. angewendet.

Das sind nur einige (wenige) Optionen und Aktionen, welche hauptsächlich zur "reinen" Filterung angewendet werden. iptables kennt noch viele weitere Optionen und Möglichkeiten, welche **hier** kurz beschrieben werden.

Policies

Aufgrund der Vielzahl von Möglichkeiten kann man nicht für jedes mögliche Paket (d.h. Kombination aus Protokoll, Netzwerkschnittstelle, Port etc.) eine Filterregel aufstellen. Daher kann für jede Chain eine sogenannten Policy (frei übersetzt: Grundsatzregel) definiert werden. Die Policy wird immer dann angewendet, wenn keine andere Filterregel zutrifft.

Die Policy setzt sich in der Regel aus dem Tabellennamen (optional), der Chain und der Aktion zusammen. Ein Beispiel:

```
iptables -P INPUT DROP
```

Hier wird festgelegt, dass für die Tabelle "filter" (im Befehl nicht explizit erwähnt, da Standard) alle eingehenden Pakete nicht angenommen werden, sofern sie keiner Filterregel entsprechen.

Weitere Optionen und Möglichkeiten

Neben den oben beschriebenen Funktionen können mit Hilfe von iptables noch viele andere Regeln und Aktionen für Netfilter erstellt werden. So beherrscht iptables / Netfilter z.B. auch "stateful inspection", d.h. Pakete werden in Abhängigkeit vom Zustand der Verbindung geprüft. "Zustand der Verbindung" bedeutet, ob das Paket z.B. zu einer bestehenden Verbindung gehört (also ein "Folgepaket" ist) oder ob es sich um eine neue Verbindung handelt. Weiterhin lassen sich mit iptables in Abhängigkeit vom Paket (bzw. der Paketprüfung) Sprünge in andere Chains realisieren. Außerdem können mit iptables eine Vielzahl von Paketmanipulationen durchgeführt werden.

Eine sehr ausführliche Übersicht und Anleitung geben die **Manpages** [https://wiki.ubuntuusers.de/man] zu iptables sowie die **Dokumentation** [http://www.iptables.org/documentation/index.html] auf der Homepage.

Einsatz von iptables

Hinweis:

In der Desktop Grundinstallation hat Ubuntu keine offenen Ports, die speziell über eine Firewall geschützt werden müssten. Weitere Informationen findet man im Artikel **Sicherheit** und **Personal Firewalls**.

Achtung!

Zu bedenken ist, dass unter Linux auch ein Teil der Interprozesskommunikation über das (interne) Netzwerk läuft, nämlich über die Netzwerkschnittstelle "lo" (z.B. **XServer** oder **CUPS**). Definiert man mit iptables Filterregel und richtet keine Regeln bzw. Policy für "lo" ein, so kann dies zu Fehlfunktionen bis hin zum Absturz des Systems führen!

Im ersten Beispiel wird überprüft, welche Filterregeln bereits hinterlegt sind. In der Grundinstallation von Ubuntu sollte hier nichts auftauchen:

```
sudo iptables -t filter -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
sudo iptables -t nat -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

```
sudo iptables -t mangle -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
```

```
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
sudo iptables -t raw -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Im zweiten Beispiel wird eine rudimentäre Firewall mit iptables aufgebaut. Dazu werden für die Netzwerkschnittstelle eth0 die Ports und Protokolle für http und https freigegeben.

Hinweis:

In der Datei **/etc/services** befindet sich eine vollständige Liste aller (systemspezifischen) Ports und der zugehörigen Protokolle.

```
iptables
-F                                                                    #alle
Regeln löschen
iptables -P INPUT
DROP                                                          #Policy für
Tabelle filter, INPUT Chain
iptables -P OUTPUT
DROP                                                          #Policy für
Tabelle filter, OUTPUT Chain
```

Es handelt sich hier um ein Beispiel und keine vollständig eingerichtete Firewall!

Hinweis:

Die mit iptables erstellten Regeln sind flüchtig, d.h. sie bleiben nur bis zum Ausschalten des Computers erhalten! Will man dauerhaft Regeln einrichten, so sollten diese in einem entsprechenden Skript hinterlegt werden, das bei Systemstart automatisch gestartet wird (siehe hierzu **rc.local** und / oder **Upstart**).

Sehr vereinfacht wird das Erstellen und Verwalten von iptables Regeln mit fertigen

Konfigurationswerkzeugen wie z.B. **firehol**.

Graphische Benutzeroberfläche

Die richtige Konfiguration von iptables auf der Kommandozeile ist sicherlich alles andere als trivial oder übersichtlich, insbesonders wenn man komplexere Regelwerke erstellen möchte (z.B. für einen Netzwerkrouter, der ggf. auch noch Firewall-Funktionalität haben soll).

Es gibt jedoch eine Reihe von (teilweise graphischen) Benutzeroberflächen, die diese Arbeit mit iptables erleichtern. So sind z.B. folgende Oberflächen über die Paketverwaltung [1] von Ubuntu verfügbar:

- **firehol** [http://packages.ubuntu.com/firehol]
- **firestarter** [http://packages.ubuntu.com/firestarter] (grafische Oberfläche, benötigt sudo-Rechte; siehe auch **Firestarter** [https://wiki.ubuntuusers.de/Firestarter])
- **guidedog** [http://packages.ubuntu.com/guidedog]
- **kmyfirewall** [http://packages.ubuntu.com/kmyfirewall]
- **pyroman** [http://packages.ubuntu.com/pyroman]
- **shorewall** [http://packages.ubuntu.com/shorewall]

Links

Intern

- **ufw** [https://wiki.ubuntuusers.de/ufw] - vereinfachte Einrichtung von iptables-Regeln
- **nathelper** [https://wiki.ubuntuusers.de/Skripte/nathelper] - Perl-Skript zum Einrichten von NAT
- **anfd** [https://wiki.ubuntuusers.de/Skripte/anfd] - Perl-Skript zum Einrichten einer applikationsabhängigen Firewall
- **Router** [https://wiki.ubuntuusers.de/Router] - Einrichtung eines einfachen Routers unter Linux

Extern

- **Einführung in iptables** [http://www.pl-forum.de/t_netzwerk/iptables.html] - Relativ ausführliche Einführung in iptables
- **Netfilter / iptables** [http://de.wikipedia.org/wiki/Netfilter] - Wikipedia-Eintrag zu Netfilter und iptables
- **Iptables – Regeln zeitgesteuert** [http://blog.telpl.de/iptables-regeln-zeitgesteuert.html] - Blogbeitrag, 05/2009
- **Basic iptables howto** [https://help.ubuntu.com/community/IptablesHowTo] - Official Ubuntu Documentation, Community Help Wiki
- **The Beginner's Guide to iptables, the Linux Firewall** [http://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall]

Diese Revision [https://wiki.ubuntuusers.de/iptables2?rev=809683] wurde am 21. April 2015 22:37 von **Vlad Cohen** erstellt.

Die folgenden Schlagworte wurden dem Artikel zugewiesen: **Sicherheit** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Sicherheit], **Netfilter** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Netfilter], **Netzwerk** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Netzwerk], **Paketfilter** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Paketfilter], **Firewall** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Firewall], **Internet** [https://wiki.ubuntuusers.de/Wiki/Tags?tag=Internet]