Firewall mit iptables Rules

Grundsätzliches

Mithilfe des Userspace-Programms iptables (bzw. ip6tables) lassen sich Ketten und Regeln in Form einer Tabelle erstellen, welche dann von der im Linux-Kernel enthaltenen Firewall abgearbeitet werden.

Das Konfigurieren mittels iptables kann als eine Sicherheitsmaßnahme für sein System verwendet werden, z.B. durch Kontrolle und Einschränkung des Netzverkehrs, Zugriffssperren von Diensten, o.ä., aber auch um Netzwerkverkehr zu manipulieren (z.B. durch Weiter-/und Umleitungen, usw.).

Iptables arbeitet auf der ISO/OSI Transport- / und Vermittlungsschicht. Das bedeutet, es können nicht alle PDU's manipuliert werden: Lediglich UDP-Datagramme, TCP-Segmente und IP-Pakete. Es gibt allerdings auch Möglichkeiten, auf Data-Link Ebene MAC-Adressen Manipulation durchzuführen. Diese Fähigkeit ist für ein Routing ohnehin unabdingbar. Iptables kann eine Penetration des Systems auf Applikationsebene daher nicht verhindern: hierfür müssen andere Maßnahmen getroffen werden (Proxy/Application-Level-Gateway, ...).

Funktionsweise - Chains/Ketten

Egal, ob ein Paket vom eigenen Rechner ins Netzwerk geschickt werden soll, oder von außerhalb zum Rechner gelangt, oder aber der Rechner das Paket an der einen Stelle annehmen und einfach zur nächsten weiterleiten soll, so durchläuft dieses Paket bei iptables immer mindestens eine Chain (dt. Kette„). Davon gibt es fünf vordefinierte, wobei nicht jede Tabelle wirklich alle Chains verwendet:

- INPUT - Der Name der Kette zeigt auch schon die Funtkionsweise auf: Ein Paket wird lokal zugestellt.
- OUTPUT - Ein Paket, welches vom eigenen Rechner erzeugt wurde und weggeschickt werden soll, wird mindestens diese Chain durchlaufen.
- FORWARD - Diese Kette dient allen Paketen, welche geroutet aber nicht lokal zugestellt werden.
- PREROUTING - Pakete durchlaufen diese Chain, noch vor dem Routing.
- POSTROUTING - Pakete durchlaufen diese Kette, nachdem sie geroutet wurden, aber noch bevor sie weitergeleitet werden.

Funktionsweise - Policy

Mithilfe von iptables kann man sehr fein definieren, was mit einzelnen Paketen, welche die unterschiedlichen Ketten durchlaufen, passieren soll. So durchläuft ein Paket nacheinander alle Regeln der Kette, bis eine passende gefunden ist.

Erreicht ein Paket aber das Ende der Kette, ohne dass eine der definierten Regeln Einfluss auf das Paket genommen hat, so greift die Policy. Diese Entscheidet dann, was mit all' den Paketen geschehen soll, welche das Ende der Tabelle erreichen. Hierzu dienen meist ACCEPT (Pakete dürfen Filterkette passieren), DROP (Paket wird als ungültig verworfen) und REJECT (Paket wird verworfen und ein ICMP Paket mit einer Meldung wie „port unreachable“ wird zurückgesendet).

Wenn man also z.B. alle eingehenden Pakete, auf welche keine Regel zutrifft, verwerfen möchte, so würde das wie folgt aussehen:

```
# iptables -P INPUT DROP
```

Funktionsweise - Regeln

Regeln werden in jeder Chain aufgestellt und können Pakete unterschiedlicher Protokolle, Herkunft, Ziele, usw. betreffen.

Ein Paket durchläuft von der 1. Regel, bis zur leztzten Regel solange die Kette, bis eine Regel auf das Paket zutrifft, oder das Ende der Kette erreicht ist. In letzterem Fall greift dann die oben beschriebene Policy.

```
# iptables -A INPUT -s 192.168.178.5 -p icmp -j ACCEPT
# iptables -A INPUT -s 192.168.178.61 -p icmp -j DROP
```

in diesem Beispiel, würde ein ICMP-Paket, welche von dem Host mit der IP-Adresse 192.168.178.5 stammt, akzeptiert werden. Das Paket würde an dieser Stelle die Kette verlassen und dürfte passieren. Ein ICMP-Paket, welches von der Adresse 192.168.178.61 stammen würde, würde die Kette bis zur 2. Regel durchlaufen (da die erste nicht auf das Paket zutrifft) und dann laut Regel verworfen werden.

Funktionsweise - Tabellen

Regeln und Ketten werden bei iptables in verschiedenen Tabellen zusammengefasst. Diese Tabellen dienen grundlegenden Aufgaben:

Tabelle	**Aufgabe**
Filter	Die Standardtabelle von iptables. Dient der reinen Paketfilterung. Beinhaltet die Ketten INPUT, OUTPUT, FORWARD.
NAT	Diese Tabelle wird für Adressumsetzung und Routing benötigt. Beinhaltet die Ketten PRE-/POSTROUTING und FORWARD.
MANGLE	Dient der Paketmodifikation. Beinhaltet PRE-/POSTROUTING, FORWARD, INPUT und OUTPUT.
RAW	Paket durchläuft Ketten dieser Tabelle als Erstes. Dient dazu um Ausnahmen vom Connection Tracking zu definieren oder Pakete mittels TRACE-Kette zu verfolgen. Beinhaltet die Ketten TRACE, PREROUTING, OUTPUT.

Grundlegende Parameter

Hier einmal ein paar grundlegende Parameter, um iptables zu konfigurieren:

Parameter	Beschreibung
-N	Legt eine neue Kette an
-X	Löscht eine leere, selbsterstellte Kette
-P	Ändert die Policy einer Kette
-F	Löscht alle Regeln aus einer Kette
-Z	Paket- und Bytezähler aller Regeln einer Kette = 0
-L	Auflisten aller Regeln
-A	Eine neue Regel in einer Kette erstellen
-I	Eine neue Regel in einer bestimmten Position einfügen
-R	Eine Regel an eine bestimmte Position in der Kette ersetzen
-D <Nummer>	Eine Regel an einer bestimmten Position in einer Kette löschen
-D	Die erste passende Regel in einer Kette löschen

iptables Regeln dauerhaft speichern

Dieser Abschnitt zeigt verschiedene Möglichkeiten, wie iptables Rules unter Linux dauerhaft gespeichert werden können.

```
# iptables-save
```

Die eigentlichen iptables Rules werden auf der Kommandozeile mit dem Kommando iptables für IPv4 und ip6tables für IPv6 erstellt und angepasst. Dies geschieht über das Firewall Script /etc/init.d/firewall In eine Datei können diese mit dem Kommando iptables-save für IPv4 gespeichert werden.

Debian/Ubuntu:

```
# iptables-save > /etc/iptables/rules.v4
```

Diese Datei kann danach wieder mit dem Kommando iptables-restore für IPv4 geladen werden.

Debian/Ubuntu:

```
# iptables-restore < /etc/iptables/rules.v4
```

Wenn auch IPv6 Regeln verwenden möchten, können diese ebenso in eine eigene Datei gespeichert werden.

Debian/Ubuntu:

```
# iptables-save > /etc/iptables/rules.v6
```

Das automatische Laden der konfigurierten iptables Rules kann mit folgenden Methoden bewerkstelligt werden:

iptables-persistent für Debian/Ubuntu

Seit Ubuntu 10.04 LTS (Lucid) und Debian 6.0 (Squeeze) gibt es ein Paket namens „iptables-persistent“ welches das automatische Laden der gespeicherten iptables Rules übernimmt. Dafür müsssen die Rules in der Datei /etc/iptables/rules.v4 für IPv4 und in /etc/iptables/rules.v6 für IPv6 gespeichert werden.

Für die Verwendung muss lediglich das Paket installiert werden.

```
# apt-get install iptables-persistent
```

Ältere iptables-persistent Versionen (z.b. jene bei Debian Squeeze) unterstützen noch keine IPv6 Rules. Dort gibt es nur eine Datei namens /etc/iptables/rules für IPv4. Wichtig!!! Prüfe nach erfolgter Konfiguration unbedingt ob die Rules wie gewünscht nach einem Reboot geladen werden.

From:
https://www.cooltux.net/ - **TuxNet DokuWiki**

Permanent link:
https://www.cooltux.net/doku.php?id=it-wiki:netzwerk:iptables&rev=1409642566

Last update: **2014/09/02 07:22**