Häufig verwendete Iptables-Optionen

Kommandos:

-P (--policy) -P *chain*
Legt die Sicherheitsrichtlinie für eine fest eingebaute Kette fest. Die Sicherheitsrichtlinie bestimmt was mit einem Paket geschehen soll, wenn es eine Kette durchlaufen hat und keine passende Regel gefunden wurde.

-A (--append) -A *chain*
Fügt einer Kette eine Regel hinzu (am Ende).

-F (--flush) -F *[chain]*
Alle Regeln einer Kette werden gelöscht. Wird keine spezielle Kette angegeben werden die Regeln aller Ketten gelöscht.

-N (--new-chain) - N *chain*
Eine neue benutzerdefinierte Kette wird erstellt.

-X (--delete-chain) -X *[chain]*
Löscht eine benutzerdefinierte Kette. Die Kette darf keine Regeln mehr beinhalten. Wird keine benutzerdefinierte Kette angegeben werden alle Ketten gelöscht. Fest eingebaute Ketten können nicht gelöscht werden.

-L (--list) -L *[chain]*
Gibt alle Regeln einer Kette am Bildschirm aus. Wird keine Kette angegeben werden die Regeln aller Ketten ausgegeben.

Parameter:

-t (--table) -t *table*
Wählt die jeweilige Tabelle aus. Erfolgt keine Auswahl über den Parameter -t wird standardmäßig die Tabelle *filter* ausgewählt. In der Regel werden alle Operationen über diese Tabelle erfolgen. Die Tabelle *filter* enthält die fest eingebauten Ketten INPUT, OUTPUT und FORWARD. Für das Maskieren der Absender-IP-Adresse wird zusätzlich die Tabelle *nat* benötigt. Die Tabelle *nat* enthält die fest eingebauten Ketten PREROUTING, POSTROUTING und OUTPUT.

-p (--protocol) -p [!] *protocol*
Erwartet die Angabe eines Protokolls wie tcp, udp oder icmp.

--dport (--destination-port) --dport [!] *port[:port]*
In Verbindung mit *-p tcp* oder *-p udp*, kann der Zielport als Portnummer oder als Name angegeben werden. Eine Übersicht der Zuordnung von Namen und Ports findet man in */etc/services*. Die Angabe eines Portbereichs ist ebenfalls möglich z. B. *1024:65535* für alle unpriviligierten Ports.

--sport (--source-port) --sport [!] *port[:port]*
Angabe des Quellports in Verbindung mit *-p tcp* oder *-p udp*.

--icmp-type

Spezifiziert den ICMP-Typ in Verbindung mit *-p icmp*. Z. B. *echo-request* oder *echo-reply*.

-i (--in-interface) -i [!] *name*
Gibt das Interface an, über welches die Pakete auf den Rechner gelangen. Z.B. *eth0* für die erste Ethernet-Netzwerkkarte oder *lo* für die Loopback-Schnittstelle.

-o (--out-interface) -o [!] *name*
Gibt an, über welche Schnittstelle die Pakete den Rechner verlassen.

-s (--source) -s [!] address[/mask]
Angabe eines speziellen Absenders. Als Absender kann ein ganzes Netz mit Angabe der Netzmaske z.B in der Form *10.0.0.0/8* oder eine einzelne IP-Adresse angegeben werden.

-d (--destination) -d [!] address[/mask]
Angabe einer bestimmten Zieladresse.

-j (--jump) -j target
Angabe eines Sprungziels. Sprungziele können z. B. sein *ACCEPT*, *DROP*, *LOG* oder eine benutzerdefinierte Kette.

-v (--verbose)
Liefert detailliertere Informationen z. B. bei der Ausgabe in Verbindung mit *-L*.

-m (--match) -m match extension
Die match extension *state* wird z.B verwendet für die Statusauswertung der Verbindung: -m state [!]--state *state* Als Status einer Verbindung kommen z. B. in Frage: NEW, ESTABLISHED, RELATED oder INVALID

Mit *iprange* kann ein ganzer IP Adressbereich angegeben werden.
-m iprange [!]--src-range *from [-to]*
-m iprange [!]--dst-range *from [-to]*

limit kann in Verbindung mit -j LOG zur Begrenzung der Logeinträge dienen: -m limit [!]--limit *rate[/second|/minute|/hour|/day]*

Mit -m mac [!]--mac-source *address* kann z.B. eine bestimmte Hardware-Absendeadresse in der Form XX:XX:XX:XX:XX.XX angegeben werden.

Es gibt eine große Anzahl weiterer match extensions, die hier nicht alle aufgeführt werden können. An dieser Stelle sei auf die Manpage von iptables verwiesen, die eine detaillierte Übersicht aller Optionen enthält.

--log-prefix Kann in Verbindung mit -j LOG verwendet werden, um dem Eintrag in die Logdatei einen Text hinzuzufügen. Der Text muss dabei in Anführungszeichen gesetzt werden.