Bild 10

```
root@antichrist:/home/wachbirn$
zerst denkn,dann tippn-# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
LOG        all  --  anywhere             anywhere             LOG level debug prefix "*INPUT*  DROP "

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

Bild 11

```
root@antichrist:/etc/iptables$
zerst denkn,dann tippn-# ls -l
insgesamt 20
-rw-r--r-- 1 root root 1145 Dez 30 14:05 rules.v
-rw-r--r-- 1 root root 1109 Jän 11 17:13 rules.v4
-rw-r--r-- 1 root root 1106 Jän 11 17:12 rules.v4_aktuell_2017
-rw-r--r-- 1 root root  200 Jul 14  2016 rules.v4_orig
-rw-r----- 1 root root    0 Sep 23 16:10 rules.v6
-rwxr-xr-x 1 root root 1219 Sep 30 17:28 standalone-firewall.sh*
```

Bild 12

```
25 *filter
26 :INPUT DROP [0:0]
27 :FORWARD ACCEPT [0:0]
28 :OUTPUT ACCEPT [31541:2842577]
29 -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
30 -A INPUT -i lo -j ACCEPT
31 -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
32 -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
33 -A INPUT -j LOG --log-prefix "*INPUT*  DROP " --log-level 7
34 COMMIT
35 # Completed on Wed Jan 11 17:13:44 2017
/etc/iptables/rules.v4[unix][conf][100%][35,1]
```

Bild 13

```
root@antichrist:/etc/iptables$
zerst denkn,dann tippn-# journalctl |grep "*INPUT"
Jän 16 14:46:13 antichrist kernel: *INPUT*  DROP IN=wlan0 OUT= MAC=00:21:6a:9e:c5:84:dc:e
68.43.1 DST=192.168.43.44 LEN=131 TOS=0x00 PREC=0x00 TTL=64 ID=30618 DF PROTO=UDP SPT=53 DPT=45471 LEN=111
Jän 16 14:46:13 antichrist kernel: *INPUT*  DROP IN=wlan0 OUT= MAC=00:21:6a:9e:c5:84:dc:ee:06:c1:e3:cc:08:00
68.43.1 DST=192.168.43.44 LEN=131 TOS=0x00 PREC=0x00 TTL=64 ID=30619 DF PROTO=UDP SPT=53 DPT=46224 LEN=111
Jän 16 15:20:41 antichrist kernel: *INPUT*  DROP IN=wlan0 OUT= MAC=ff:ff:ff:ff:ff:ff:08:00:27:c2:6e:5c:08:00
.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
Jän 16 15:20:41 antichrist kernel: *INPUT*  DROP IN=wlan0 OUT= MAC=ff:ff:ff:ff:ff:ff:dc:ee:06:c1:e3:cc:08:00
68.43.1 DST=255.255.255.255 LEN=337 TOS=0x00 PREC=0x00 TTL=64 ID=11279 PROTO=UDP SPT=67 DPT=68 LEN=317
Jän 16 15:20:41 antichrist kernel: *INPUT*  DROP IN=wlan0 OUT= MAC=ff:ff:ff:ff:ff:ff:08:00:27:c2:6e:5c:08:00
.0 DST=255.255.255.255 LEN=328 TOS=0x10 PREC=0x00 TTL=128 ID=0 PROTO=UDP SPT=68 DPT=67 LEN=308
```

Falls Dienste im Internet angeboten werden, kommt man freilich um diesen Paketfilter nicht mehr herum. Entweder am Router, auf der Maschine selbst, auf einer eigenen Maschine oder mit einer Mischung aus allem zusammen. Kommt immer drauf an.

Als normaler Anwender zu Hause… vergiss das. Unnötig. Falls Du aber nicht mehr an Deiner geliebten Wasserstoffbombe weiterbasteln willst, kannst Du natürlich auch den Paketfilter als Dein neues Hobby betrachten. Wie sieht sowas aus? Keine Ahnung, ich zeig Dir mal meine Konfiguration. **Siehe Bild 10.**

Ja, ich weiß, die „schönsten Nebenbahnstrecken der Welt“ in der Glotze um drei in der Früh sind aufregender. `iptables -L` listet mir mal die Übersicht auf. Für die Profis: Ich will da jetzt nicht zu sehr ins Detail auf die verschiedenen Ketten und Policys gehen, sondern das Ganze so verständlich wie möglich auch für Uneingeweihte machen.

Also, woher kommt die ganze Ausgabe? Du schreibst die Regeln in die Kommandozeile und speicherst die dann. Fertig.

Wenn Du die Regeln ändern willst, schreibst Du das genauso in der Kommandozeile rein. Fertig. Die Änderungen werden augenblicklich übernommen. *On the fly*. Ja, stimmt. Die Syntax der Regeln musst Du einmal lernen oder Du nimmst eine grafische Lösung.

Diese Regeln kann man sich im entsprechenden Konfigurationsfile auch anschauen. Unter `/etc/iptables` (o wunder) gibt’s folgende Files. **Siehe Bild 11.**

`rulesv4` steht für Internetadresse Ipv4. Gibt auch Ipv6, interessiert mich aber derweil nicht wirklich, da ich auf meiner Maschine Ipv6 sowieso deaktiviert habe. Der Hauptunterschied zwischen den zwei Klassen besteht in der Größenordnung. 32 zu 128bit eben. vier Milliarden mögliche Adressen zu… *woswasi… füh hoit*.

Was steht da drin in dem File? Das was bei der Ausgabe unter **Bild 10** rauskommt. **Siehe Bild 10 - 12.**

Alles, was reinkommt von außen, wird in der Regel verworfen. Das ist die Standardpolicy. `INPUT:DROP [0:0]`

Die Nullen stehen für die Maschine und fürs Display. Egal jetzt.

Die Policy setze ich auf der Kommandozeile so > „`iptables -P INPUT DROP`“.

Alles, was durch-oder weitergeleitet werden soll, definiere ich eben. Siehe Zeile 29 bei **Bild 12**. Alle internen Schnittstellen (127er Adressen) sind freigeschalten. Zeile 30. Pings sind auch freigeschalten auf meine Maschine > Zeile 31. SSH ist auch freigeschalten auf Port 22. Zeile 32. Alle verworfenen Pakete werden protokolliert. Zeile 33. Das Ergebnis siehst Du dann auf **Bild 10**. Alles, was nicht auf die paar Regeln passt, wird verworfen > Input Policy drop.

Alles, was jetzt verworfen wurde, kann ich mit dem Kommando (gelb unterstrichen) auf **Bild 13** einsehen. In rot sind die ver-

Ich muss zugeben, für mich war vieles von dem auch Neuland. Als Hauptverantwortliche dieses Umstandes konnte ich zweifelsfrei die kulturelle Prägung und die ubiquitäre Fantasielosigkeit meinerseits ausmachen. Seitdem stehe ich in einem ständigen Dialog mit mir und kann Dir beruhigt versichern, wir schenken uns nichts.

Die heutzutage obligatorische Demo gegen rechts am Breitscheidplatz in Berlin nach dem LKW-Attentat entlockt mir nicht mal mehr ein müdes Lächeln. Mittlerweile könnte man schon den Eindruck gewinnen, dass die Besorgnis über die Instrumentalisierung der Tat bedeutend schwerer als Selbige wiegt.

Das erinnert mich immer an eine Szene aus einem lustigen Spielfilm, wo sich Leute nach einem Erdbeben auf den Seismographen als Schuldigen einigen und postwendend zerstören.

Zudem stülpt man mit dem im „psychischen Ausnahmezustand“ befindlichen Attentäter ganz entspannt den psychisch Kranken einen jovialen Generalverdacht über. Und obendrein da auch nur den Männern. Sind jetzt alle psychisch Kranken Terroristen oder gewaltaffin? Merkst Du gar nicht, dass Du dich diskriminierenderweise auf recht dünnem Eis bewegst? Ist das schon wieder Hetze? Werden durch diese Frage nicht automatisch die adipösen Eisberge stigmatisiert?

Ähhh, wo war ich gerade? Okay, die haben jetzt nicht die Mörder-Lobby hinter sich, aber mit welcher Nonchalance da gewissen Minderheiten extreme Gewaltverbrechen pauschalmäßig zugeordnet werden, da kann man nur staunen.

In Bataclan wurde demgegenüber zur einjährigen Gedenkfeier des Anschlages die damals auftretende Band wegen kritischer Aussagen von der Zeremonie ausgeschlossen. Geht doch. Man muss schon differenzieren können.

Auch wurde ein neuer Arbeitsplatz erschaffen. Kurt Beck hat in Deutschland jetzt den Posten des „Beauftragten für Opfer und Hinterbliebene“ ergattert. So sollen zukünftige Opfer von Terroranschlägen einen kompetenten Ansprechpartner erhalten.

Mittlerweile wird nach den Terroranschlägen immer das selbe Muster abgespielt.

1.Ein Anschlag passiert

2.#pray for ……

3.je suis…

4.eventuell noch cartoons

5.Avatar in Landesfarben einfärben

6.Terrorismus Experte erklärt alles… auch das mit der diffusen Angst

7.Kabarettisten „jetzt erst recht… machen weiter, sicherheitshalber ohne Religionswitze… “

8.Demo gegen rechts