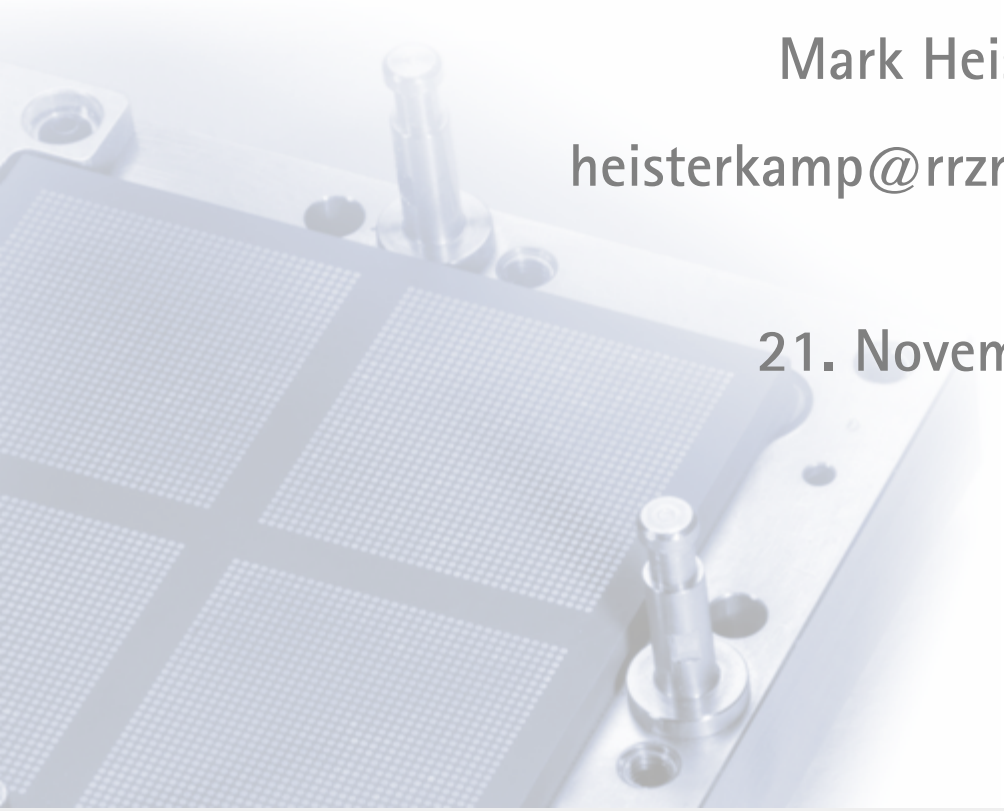
Mac OS X Firewall

Mark Heisterkamp

heisterkamp@rrzn.uni-hannover.de

21. November 2011



Lion

Seit Mac OS X 10.7 drei Firewalls:

- Applikationsspezifisch
- pf (OpenBSD)
- ipfw (Free-BSD, *deprecated*)

Drei Konfigurationspunkte

- Systemeinstellungen → Freigaben
- Systemeinstellungen → Sicherheit → Firewall
- Kommandozeile

Leibniz Universität Hannover

Auslieferungszustand – netstat

```
netstat -a|grep LISTEN

tcp4       0      0  *.ms-v-worlds          *.*    LISTEN
tcp46      0      0  *.5204                 *.*    LISTEN
tcp4       0      0  *.5204                 *.*    LISTEN
tcp4       0      0  localhost.ipp          *.*    LISTEN
tcp6       0      0  localhost.ipp          *.*    LISTEN
```

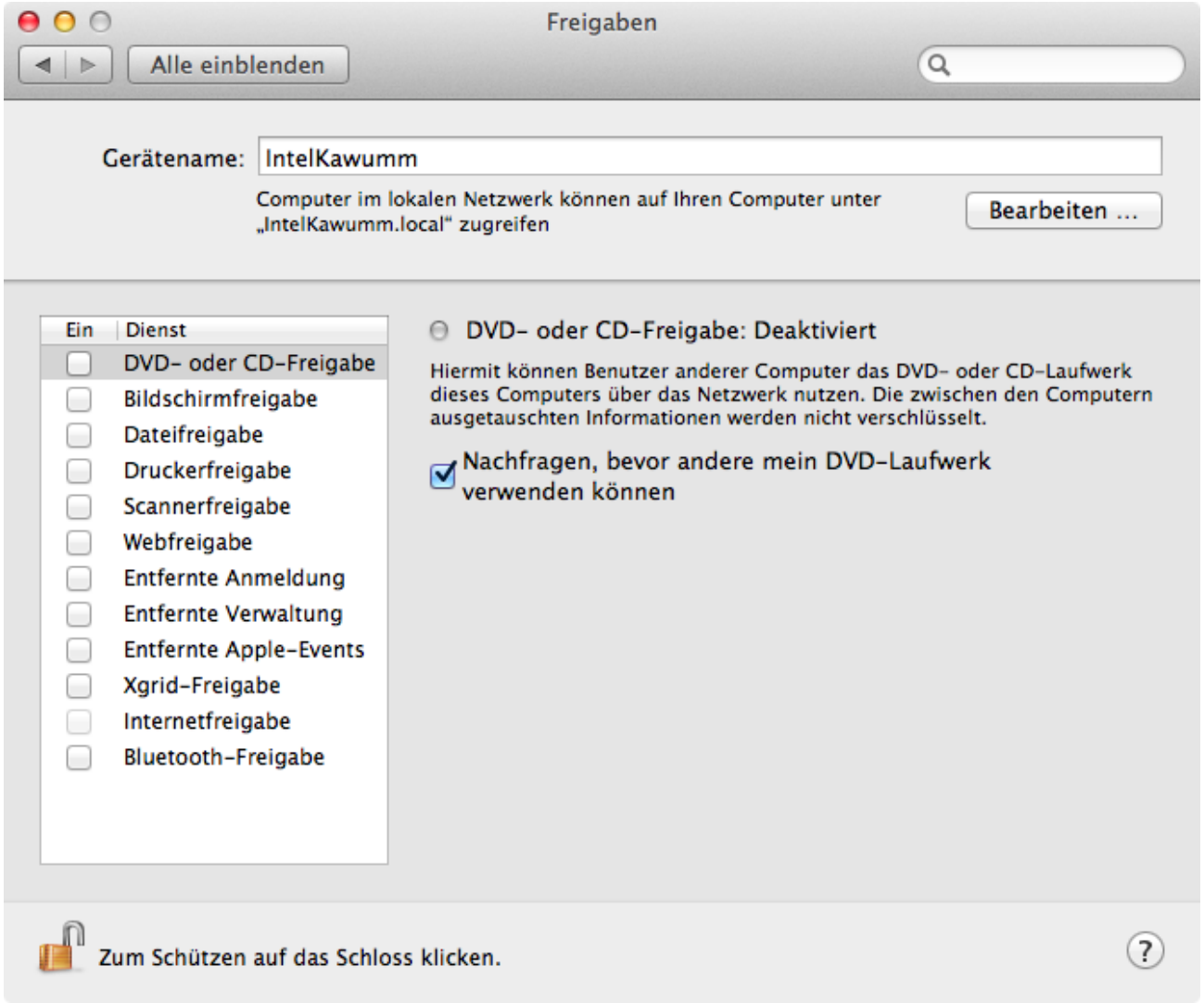
Auslieferungszustand – lsof

```
sudo lsof|grep LISTEN

launchd       1            root   19u   TCP ip6-localhost:ipp (LISTEN)
launchd       1            root   20u   TCP localhost:ipp (LISTEN)
iStatLoca    55            root    4u   TCP *:5204 (LISTEN)
iStatLoca    55            root    7u   TCP *:5204 (LISTEN)
tina_daem   984            root    5u   TCP *:ms-v-worlds (LISTEN)
```

Portscan – nmap

```
nmap -PN 192.168.0.147

Starting Nmap 5.00 ( http://nmap.org ) at ...
Interesting ports on 192.168.0.147:
Not shown: 999 closed ports
PORT     STATE SERVICE
2525/tcp open  unknown
MAC Address: 00:22:41:27:0A:62 (Apple)
```

Freigaben


Freigaben
Alle einblenden
Gerätename: IntelKawumm
Computer im lokalen Netzwerk können auf Ihren Computer unter „IntelKawumm.local“ zugreifen
Bearbeiten ...
Ein
Dienst
DVD- oder CD-Freigabe
Bildschirmfreigabe
Dateifreigabe
Druckerfreigabe
Scannerfreigabe
Webfreigabe
Entfernte Anmeldung
Entfernte Verwaltung
Entfernte Apple-Events
Xgrid-Freigabe
Internetfreigabe
Bluetooth-Freigabe
DVD- oder CD-Freigabe: Deaktiviert
Hiermit können Benutzer anderer Computer das DVD- oder CD-Laufwerk dieses Computers über das Netzwerk nutzen. Die zwischen den Computern ausgetauschten Informationen werden nicht verschlüsselt.
Nachfragen, bevor andere mein DVD-Laufwerk verwenden können
Zum Schützen auf das Schloss klicken.

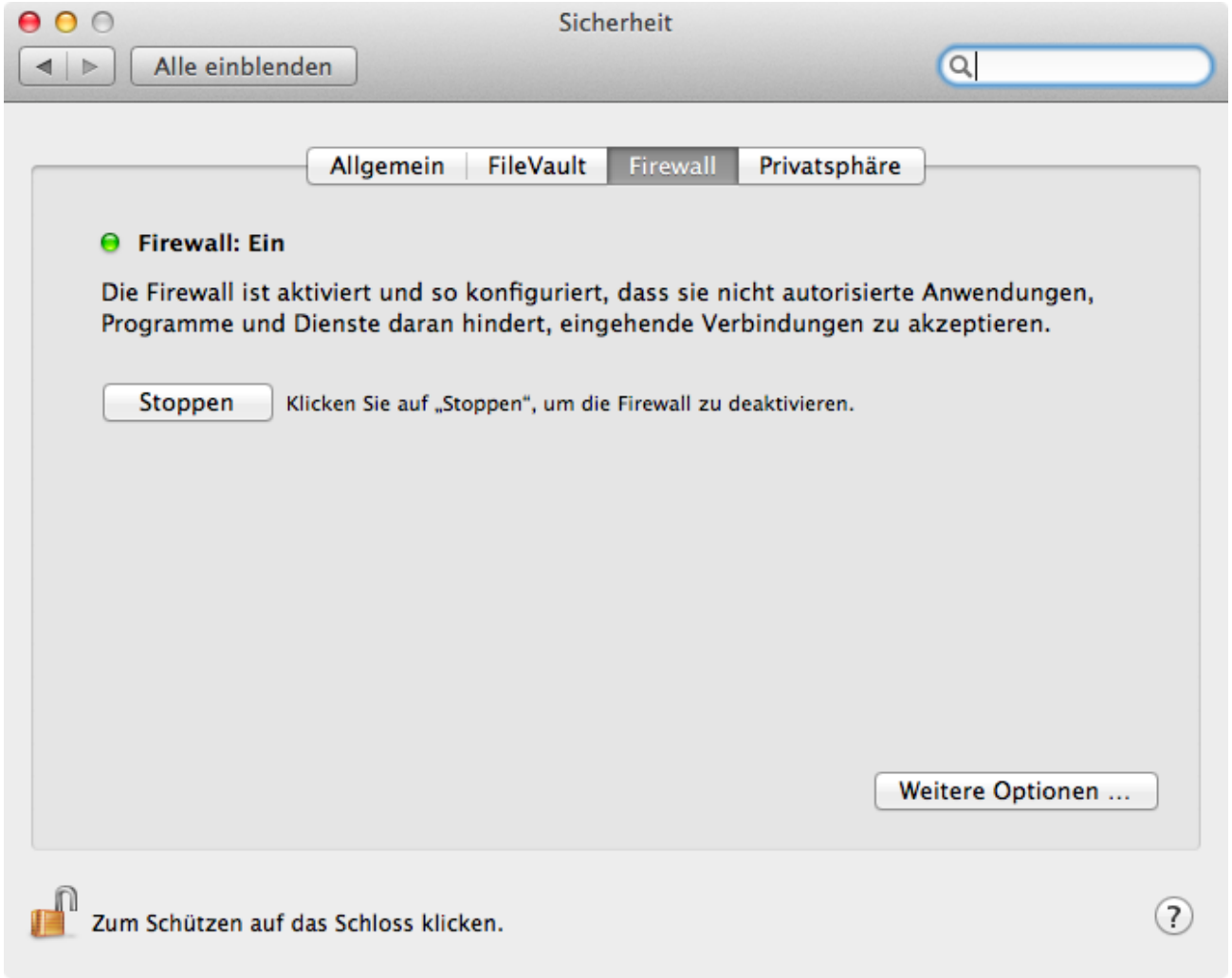
Leibniz Universität Hannover

Auslieferungszustand – netstat

```
sudo netstat -a|grep LISTEN

tcp6       0      0  *.ssh                  *.*    LISTEN
tcp4       0      0  *.ssh                  *.*    LISTEN
tcp6       0      0  *.ipp                  *.*    LISTEN
tcp4       0      0  *.ipp                  *.*    LISTEN
tcp4       0      0  *.ms-v-worlds          *.*    LISTEN
tcp46      0      0  *.5204                 *.*    LISTEN
tcp4       0      0  *.5204                 *.*    LISTEN
tcp4       0      0  localhost.ipp          *.*    LISTEN
tcp6       0      0  ip6-localhost.ipp      *.*    LISTEN
```

Applikationsfirewall – aus

Applikationsfirewall – an



Applikationsfirewall – an

pf – der Letzte lacht am besten

Es werden alle Regeln für ein Paket abgearbeitet, die letzte zutreffende Regel gilt!

```
block in all
pass in all
```

Lässt sämtlichen eingehenden Verkehr durch.

pf – pfctl

- *pf* einschalten:

```
sudo pfctl -e
```

- *pf* ausschalten:

```
sudo pfctl -d
```

- Konfigurationsdatei:

```
/etc/pf.conf
```

pf – pf.conf

/etc/pf.conf besteht aus sieben Abschnitten:

Makros	– Variablendefinitionen zur einfacheren Strukturierung
Tabellen	– Sammlungen von Netzwerkadressen
Optionen	– Feinjustierung von *pf*
Paketnormalisierung	– (*scrubbing*) Defragmentierung, Drop ungültiger Pakete
Queueing	– Bandbreitenanpassungen
NAT	– …
Paketfilter	– Eigentliche Firewall-Regeln

Leer- und Kommentarzeilen (#) werden ignoriert. Die Reihenfolge der Abschnitte muss eingehalten werden!

Leibniz Universität Hannover

Einige simple Kommandos

`pfctl -f /etc/pf.conf` – Lädt die pf.conf-Datei

`pfctl -nf /etc/pf.conf` – Analysiert die Datei, aber lädt sie nicht

`pfctl -Nf /etc/pf.conf` – Lädt nur die NAT-Regeln der Datei

`pfctl -Rf /etc/pf.conf` – Lädt nur die Filterregeln der Datei

`pfctl -sn` – Zeigt die aktuellen NAT-Regeln

`pfctl -sr` – Zeigt die aktuellen Filterregeln

`pfctl -ss` – Zeigt die aktuelle Statustabelle

`pfctl -si` – Zeigt Filterstatistiken und Zähler

`pfctl -sa` – Zeigt ALLES was gezeigt werden kann

Meine bisherigen Regeln – ipfw

```
sudo ipfw list
00800 allow ip from any to any via lo*
01300 allow ip from any to any out keep-state
01400 allow udp from any 67 to any dst-port 68 in
01600 allow tcp from any to me dst-port 22 in keep-state
01710 allow tcp from 130.75.6.22,130.75.6.23 to me dst-port 2525
01720 allow udp from 130.75.6.22,130.75.6.23 to me dst-port 2526
01900 allow icmp from any to me in icmptypes 8 keep-state
65534 deny ip from any to any
65535 allow ip from any to any
```

Meine jetzigen Regeln – pf

```
sudo mv /etc/pf.conf /etc/pf.conf.orig
sudo vi /etc/pf.conf

scrub in all fragment reassemble
block in all
pass out all
set skip on lo0
pass in on {en0,en1} proto udp from any port bootps to any port bootpc
pass in proto tcp to port ssh
pass in on en0 proto tcp from {130.75.6.22,130.75.6.23} to port 2525
pass in on en0 proto udp from {130.75.6.22,130.75.6.23} to port 2526
pass in inet proto icmp all icmp-type echoreq
```

Firewall beim Boot aktivieren

```
sudo vi /System/Library/LaunchDaemons/com.apple.pfctl.plist
```

Zeile hinzufügen:

```
<string>-e</string>
```

```
...
        <array>
                <string>pfctl</string>
                <string>-f</string>
                <string>/etc/pf.conf</string>
                <string>-e</string>
        </array>
...
```

pf Aktiviert? – Ja!

```
sudo pfctl -sr

No ALTQ support in kernel
ALTQ related functions disabled
scrub in all fragment reassemble
block drop in all
pass in on en0 proto udp from any port = 67 to any port = 68 keep state
pass in on en1 proto udp from any port = 67 to any port = 68 keep state
pass out all flags S/SA keep state
pass in on en0 inet proto tcp from 130.75.6.22 to any port = 2525 flags S/SA \
  keep state
pass in on en0 inet proto tcp from 130.75.6.23 to any port = 2525 flags S/SA \
  keep state
pass in proto tcp from any to any port = 22 flags S/SA keep state
pass in on en0 inet proto udp from 130.75.6.22 to any port = 2526 keep state
pass in on en0 inet proto udp from 130.75.6.23 to any port = 2526 keep state
pass in inet proto icmp all icmp-type echoreq keep state
```

Links

- Das Original:
  http://openbsd.org/faq/pf/de/index.html
- Heise-Meldung mit kurzer Einführung:
  http://www.heise.de/netze/artikel/Das-Firewall-Tool-pf-in-Mac-OS-X-10-7-Lion-1348566.html