

# Mac Firewall etc.

Mark Heisterkamp

heisterkamp@rrzn.uni-hannover.de

10. August 2009

# Leopard

Seit Mac OS X 10.5 zwei Firewalls:

- Applikationsspezifisch
- ipfw (Free-BSD)

Wobei ipfw maßgeblich ist. Jede **ipfw-Beschränkung** gilt unabhängig von der Applikations-Firewall.

# Applikationsspezifisch

The screenshot shows the 'Sicherheit' (Security) window in Mac OS X, specifically the 'Firewall' tab. The window title is 'Sicherheit'. At the top left, there are window control buttons and a search field. Below the title bar, there are three tabs: 'Allgemein', 'FileVault', and 'Firewall'. The 'Firewall' tab is selected. The main content area contains three radio button options: 'Alle eingehenden Verbindungen erlauben' (selected), 'Nur notwendige Dienste erlauben', and 'Zugriff für bestimmte Dienste und Programme festlegen'. Below these options is a paragraph of text: 'Normalerweise bestimmt Mac OS X, für welche Programme eingehende Verbindungen erlaubt sind. Wählen Sie diese Option aus, wenn Sie eingehende Verbindungen für bestimmte Programme erlauben oder blockieren möchten.' Below this text is a list box titled 'Web-Sharing' and 'Entfernte Anmeldung (SSH)'. The list contains four entries: 'perl', 'Cyberduck.app', 'VirtualBoxVM', and 'iTunes.app'. Each entry has a corresponding action: 'Eingehende Verbindungen blockieren'. At the bottom of the list box are '+' and '-' buttons. To the right of the list box is a button labeled 'Weitere Optionen ...'. At the bottom left of the window is a lock icon and the text 'Klicken Sie auf das Schloss, um Änderungen zu verhindern.' At the bottom right is a question mark icon.

Sicherheit

Alle einblenden

Allgemein FileVault Firewall

Alle eingehenden Verbindungen erlauben

Nur notwendige Dienste erlauben

Zugriff für bestimmte Dienste und Programme festlegen

Normalerweise bestimmt Mac OS X, für welche Programme eingehende Verbindungen erlaubt sind. Wählen Sie diese Option aus, wenn Sie eingehende Verbindungen für bestimmte Programme erlauben oder blockieren möchten.

Web-Sharing  
Entfernte Anmeldung (SSH)

perl	Eingehende Verbindungen blockieren
Cyberduck.app	Eingehende Verbindungen blockieren
VirtualBoxVM	Eingehende Verbindungen blockieren
iTunes.app	Eingehende Verbindungen blockieren

+ - Weitere Optionen ...

Klicken Sie auf das Schloss, um Änderungen zu verhindern. ?

# ipfw

```
sudo ipfw disable firewall
```

```
mheiste@IntelKawumm:~>sudo ipfw list
01400 allow ip from any to any via lo*
01500 allow tcp from me to any out keep-state
01600 allow tcp from any to me dst-port 22 in keep-state
01700 allow tcp from 130.75.6.20 to me dst-port \
13720,13722,13724,13782,13783 in keep-state
01900 allow icmp from any to me in icmptypes 8 keep-state
65534 deny tcp from any to any
65535 allow ip from any to any
```

# WaterRoof (ipfw-Frontend)

rule n.	rule action	packets	bytes
01400	allow ip from any to any via lo*	15658	13872
01500	allow tcp from me to any out keep-state	3372703	12602087
01600	allow tcp from any to me dst-port 22 in keep-state	25	12
01700	allow tcp from 130.75.6.20 to me dst-port 13720,13722,13724,1378...	20102020	187757422
01900	allow icmp from any to me in icmptypes 8 keep-state	2	2
02000	allow tcp from 169.254.2.0/24 to 169.254.2.0/24 dst-port 5678,5679...	0	0
65534	deny tcp from any to any	20738	9414
65535	allow ip from any to any	86926	136257

# Port 80 – WaterRoof

**Add new rule**

Static rule number: 2000    Protocol: tcp    Rule action: allow     ipv6

**Source**  
Source address, subnet or network: any    Port or range:

**Destination**  
Destination address, subnet or network: me    Port or range: 80    Other..

**Extra**    **Log activity**    **Options**

Extra arguments:

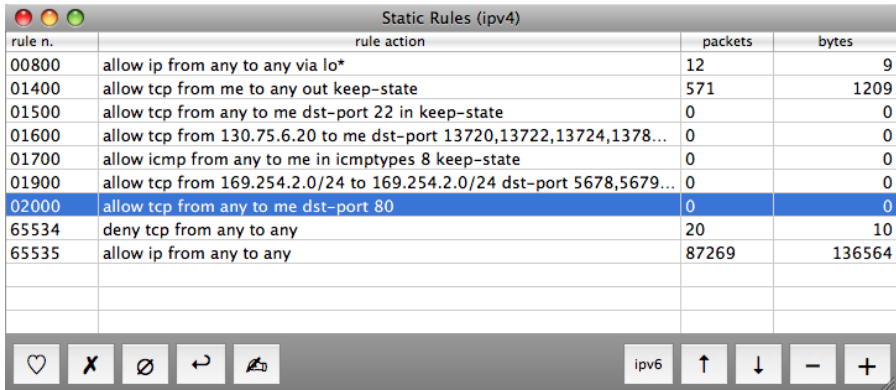
Network Interface: all

log

In     setup     bridged  
 Out     keep-state     ipsec  
 In/Out     established     User-ID

Show shell command    Network Interfaces List    ?    Add new rule

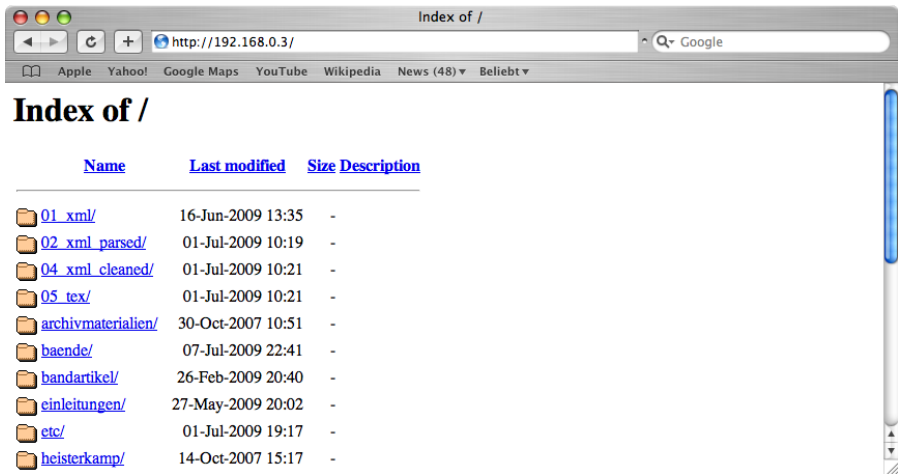
## Port 80 – WaterRoof (Ergebnis)













rule n.	rule action	packets	bytes
00800	allow ip from any to any via lo*	12	9
01400	allow tcp from me to any out keep-state	571	1209
01500	allow tcp from any to me dst-port 22 in keep-state	0	0
01600	allow tcp from 130.75.6.20 to me dst-port 13720,13722,13724,1378...	0	0
01700	allow icmp from any to me in icmptypes 8 keep-state	0	0
01900	allow tcp from 169.254.2.0/24 to 169.254.2.0/24 dst-port 5678,5679...	0	0
02000	allow tcp from any to me dst-port 80	0	0
65534	deny tcp from any to any	20	10
65535	allow ip from any to any	87269	136564

Control bar: [Heart] [X] [Empty Circle] [Undo] [Redo] [ipv6] [Up Arrow] [Down Arrow] [Minus] [Plus]

# Port 80 – Safari

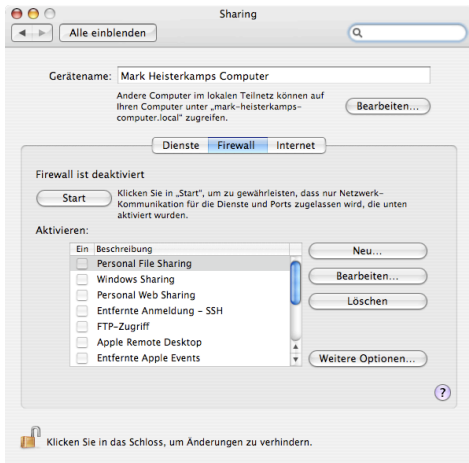


The screenshot shows a Safari browser window with the title "Index of /". The address bar contains "http://192.168.0.3/" and a search box with "Google". The browser's bookmark bar includes "Apple", "Yahoo!", "Google Maps", "YouTube", "Wikipedia", "News (48)", and "Beliebt". The main content area displays "Index of /" followed by a table of files.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">01_xml/</a>	16-Jun-2009 13:35	-	
 <a href="#">02_xml_parsed/</a>	01-Jul-2009 10:19	-	
 <a href="#">04_xml_cleaned/</a>	01-Jul-2009 10:21	-	
 <a href="#">05_tex/</a>	01-Jul-2009 10:21	-	
 <a href="#">archivmaterialien/</a>	30-Oct-2007 10:51	-	
 <a href="#">baende/</a>	07-Jul-2009 22:41	-	
 <a href="#">bandartikel/</a>	26-Feb-2009 20:40	-	
 <a href="#">einleitungen/</a>	27-May-2009 20:02	-	
 <a href="#">etc/</a>	01-Jul-2009 19:17	-	
 <a href="#">heisterkamp/</a>	14-Oct-2007 15:17	-	



# 10.4 (Tiger) ipfw-Frontend



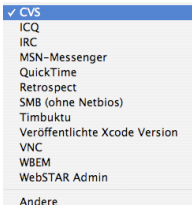
Legen Sie einen Dienst fest, für den Netzwerk-Kommunikation erlaubt werden soll. Um andere Dienste festzulegen, wählen Sie „Andere“ im Einblendmenü „Dienste“. Geben Sie dann den Namen des Dienstes und seine Port-Nummer (oder einen Bereich oder eine Folge von Nummern) zusammen mit einer Beschreibung ein.

Dienste:

TCP-Portnummer(n):

UDP-Portnummer(n):

Beschreibung:



## Tools – Frontend

- Netzwerkdienstprogramm
- Sophos  
<http://www.rrzn.uni-hannover.de/antiviren.html>
- iStat menus  
<http://www.islayer.com/apps/istatmenus/>

# Netzwerkdienstprogramm

Netzwerkdienstprogramm

Informationen Netstat AppleTalk Ping Lookup Trace Whois Finger Portscan

Bitte wählen Sie die Netzwerkschnittstelle, über die Sie Informationen erhalten möchten:

Netzwerkschnittstelle (en1)

Schnittstelleninformationen

- Hardwareadresse: 00:21:e9:e4:07:58
- IP-Adresse(n): 192.168.0.3
- Verbindungsgeschwindigkeit: 54 MBit/s
- Verbindungsstatus: Aktiv
- Hersteller: Apple
- Modell: Wireless Network Adapter (802.11 a/b/g/n)

Übertragungsstatistik

- Gesendete Pakete: 187074
- Sendefehler: 0
- Empfangene Pakete: 222123
- Empfangsfehler: 0
- Kollisionen: 0

# Netzwerkdienstprogramm – netstat

Netzwerkdienstprogramm

Informationen **Netstat** AppleTalk Ping Lookup Trace Whois Finger Portscan

Informationen der Routing-Tabelle anzeigen  
 Ausführliche Netzwerkstatistik für jedes Protokoll anzeigen  
 Multicast-Informationen anzeigen  
 Status der aktuellen Socket-Verbindungen anzeigen

Netstat

Active Internet connections (including servers)

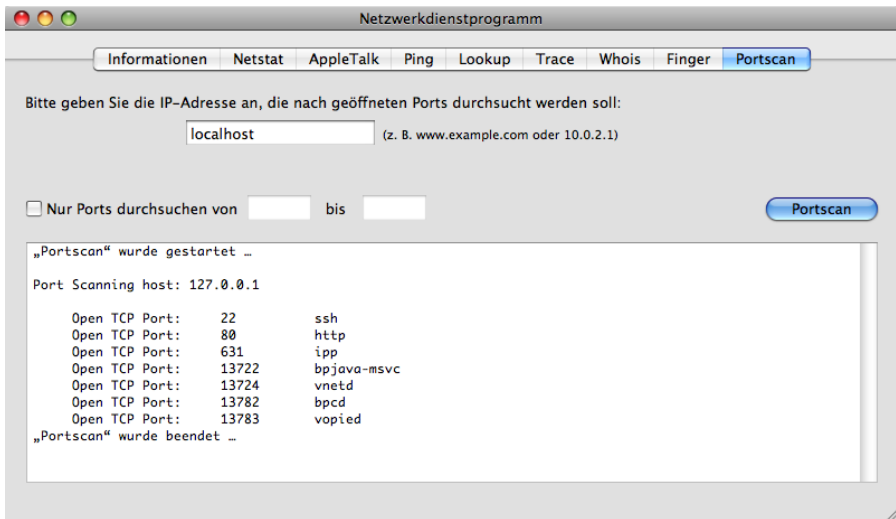
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	0	192.168.0.3.52373	buddychat-d04b.b.aol	ESTABLISHED
tcp4	0	0	192.168.0.3.52372	205.188.7.212.aol	ESTABLISHED
tcp4	0	0	192.168.0.3.52370	jabber.rrzn.uni-jabbe	ESTABLISHED
tcp4	0	0	192.168.0.3.52369	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52368	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52367	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52366	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52365	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52364	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52363	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52362	mail6240.rrzn.un.imaps	ESTABLISHED
tcp4	0	0	192.168.0.3.52361	mail6240.rrzn.un.imaps	ESTABLISHED

# Netzwerkdienstprogramm – traceroute

The screenshot shows the 'Netzwerkdienstprogramm' window with the 'Trace' tab selected. The address 'www.heise.de' is entered in the input field. The 'Trace' button is visible on the right. The output area shows the following traceroute results:

```
„Traceroute“ wurde gestartet ...  
  
traceroute to www.heise.de (193.99.144.85), 64 hops max, 40 byte packets  
1  www.routerlogin.com (192.168.0.1)  2.042 ms  1.220 ms  1.250 ms  
2  217.0.116.123 (217.0.116.123)  28.605 ms  29.815 ms  39.441 ms  
3  217.0.72.114 (217.0.72.114)  29.932 ms  29.079 ms  37.868 ms  
4  217.239.39.30 (217.239.39.30)  38.667 ms  36.568 ms  37.587 ms  
5  217.243.218.38 (217.243.218.38)  70.892 ms  131.386 ms  211.765 ms  
6  heise1.f.de.plusline.net (82.98.98.98)  43.190 ms  35.656 ms  55.511 ms  
7  heise1.f.de.plusline.net (82.98.98.98)  38.253 ms !X * 33.890 ms !X
```

# Netzwerkdienstprogramm – portscan



# Sophos

- z.Zt. 30 Viren in der Sophos-online-Datenbank
- unauffällig, praktisch



Jetzt aktualisieren

AutoUpdate Fenster anzeigen

Sophos Anti-Virus öffnen ...

Einstellungen öffnen ...

Über Sophos Anti-Virus...

# iStat menus

iStat menus

Alle einblenden

Monitor Network Usage Update every 1.0s

General Settings

Mode: Text

Format: Kilobytes, Me...

Primary: Automatic

Interfaces to monitor

AirPort

Bluetooth

Menubar Display

Show network label

Graph Width:

Menubar Text

Upload

Download

Inactive

Graph Settings

Show baseline in graphs

Show graphs in dropdown

Type: Opposed

Scaling: Linear Extreme

Graph Colors

Use custom graph colors

Upload

Download

Inactive (Menubar)

iStat menus 1.3



# Tools – Kommandozeile

## System-Tools:

- lsof
- netstat
- tcpdump

## Zusatz-Tools

- fink <http://www.finkproject.org>
  - nmap
  - iftop

## Nach Hause telefonieren ...

```
lsof -i +c0 -r
```

- i Netzwerk-Dateien anzeigen (evtl. mit IP, Hostname, Protokolltyp etc.)
- +c0 Kommandonamen ausschreiben
- r Repeat-Mode (Endlosschleife)

## netstat

Mac OS X setzt `netstat` in einer recht alten BSD-Variante ein, deren Kommandozeilenparameter sich wesentlich von der GNU-Version unterscheiden.

Insbesondere funktioniert folgendes **nicht**:

```
netstat -apW -inet -numeric-ports
```

- p PID und Kommandoname
- W Wide, nix wird abgeschnitten im Terminal
- numeric-ports Ports als Nummern

# Schöne netstat-Ausgabe (GNU)

```
heisterkamp@webdav:~$ sudo netstat -apW --inet --numeric-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:389             0.0.0.0:*                LISTEN     22069/slapd
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN     278/sshd
tcp        0      0 127.0.0.1:25           0.0.0.0:*                LISTEN     561/exim4
tcp        0      0 127.0.0.1:389         127.0.0.1:38963        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389         127.0.0.1:41420        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389         127.0.0.1:39612        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:49711       127.0.0.1:389          ESTABLISHED 28977/apache2
tcp        0      0 127.0.0.1:48855       127.0.0.1:389          ESTABLISHED 5386/apache2
tcp        0      0 127.0.0.1:389         127.0.0.1:48855        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389         127.0.0.1:43458        ESTABLISHED 22069/slapd
tcp        0      0 130.75.6.15:22        130.75.6.189:57483     ESTABLISHED 15517/ssh: heister
tcp        0      0 127.0.0.1:48857       127.0.0.1:389          ESTABLISHED 28979/apache2
tcp        0      0 127.0.0.1:389         127.0.0.1:39626        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:43458       127.0.0.1:389          ESTABLISHED 5383/apache2
tcp        0      0 127.0.0.1:39612       127.0.0.1:389          ESTABLISHED 28975/apache2
tcp        0      0 127.0.0.1:38963       127.0.0.1:389          ESTABLISHED 5384/apache2
tcp        0      0 127.0.0.1:39626       127.0.0.1:389          ESTABLISHED 5382/apache2
tcp        0      0 127.0.0.1:41420       127.0.0.1:389          ESTABLISHED 28978/apache2
tcp        0      0 127.0.0.1:389         127.0.0.1:48857        ESTABLISHED 22069/slapd
tcp        0      0 127.0.0.1:389         127.0.0.1:49711        ESTABLISHED 22069/slapd
```

# Nicht so schöne Mac-Ausgabe von netstat

```
mheiste@IntelKawumm:~>sudo netstat -a -f inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.0.3.62940      zen.rrzn.uni-han.ssh   ESTABLISHED
tcp4      0      0 192.168.0.3.62938      buddychat-d04b.b.aol   ESTABLISHED
tcp4      0      0 192.168.0.3.62937      205.188.7.212.aol     ESTABLISHED
tcp4      0      0 192.168.0.3.62935      jabber.rrzn.uni-.jabbe ESTABLISHED
tcp4      0      0 192.168.0.3.52369      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52368      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52367      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52366      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52365      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52364      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52363      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52362      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52361      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52360      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52359      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52358      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52357      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52356      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52355      mail6240.rrzn.un.imaps ESTABLISHED
tcp4      0      0 192.168.0.3.52354      mail6240.rrzn.un.imaps ESTABLISHED
```

# tcpdump

```
sudo tcpdump -i en1 -qt ip
```

- i en1 Interface 1 (Airport)
- q Quick output – kürzere Zeilen
- t Ohne Zeitstempel in jeder Zeile
- ip Protokolltyp

# tcpdump-Ausgabe

```
mheiste@IntelKawumm:~>sudo tcpdump -i en1 -qt ip
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 0
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP 192.168.0.3.63031 > www.heise.de.http: tcp 419
IP www.heise.de.http > 192.168.0.3.63031: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 8
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63031 > www.heise.de.http: tcp 0
IP 192.168.0.3.63032 > www.heise.de.http: tcp 0
IP www.heise.de.http > 192.168.0.3.63031: tcp 1440
IP 192.168.0.3.63033 > www.heise.de.http: tcp 0
```

# nmap

```
mheiste@IntelKawumm:~>nmap -P0 localhost
```

```
Starting Nmap 4.20 ( http://insecure.org ) at 2009-08-09 22:44 CEST
```

```
Interesting ports on localhost (127.0.0.1):
```

```
Not shown: 1336 closed ports, 355 filtered ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
631/tcp	open	ipp
13722/tcp	open	VeritasNetbackup
13782/tcp	open	VeritasNetbackup
13783/tcp	open	VeritasNetbackup

```
Nmap finished: 1 IP address (1 host up) scanned in 9.339 seconds
```



# sudo iftop -i en1

