IPFW

Eine einfache Firewall mit FreeBSD erstellen

Martin 'Ventilator' Ebnöther
mit viel Unterstützung von Fabian 'fab' Wenk

Vorbereitungen

Einfügen in die Kernel- Config

```
options         IPFIREWALL              # Enable ipfw
options         IPFIREWALL_VERBOSE      # Enable logging
options         IPFIREWALL_VERBOSE_LIMIT=256
                                        # Limit logging
```

Für NAT (Network Adress Translation)

```
options         IPDIVERT                # We use NAT
```

Für Bandbreitenkontrolle

```
options         DUMMYNET                # Used for bandwidth control
```

Einfügen in /etc/rc.conf

Firewallscript abarbeiten

```
firewall_enable="YES"
firewall_script="/etc/rc.firewall"
```

Routing zwischen Interfaces einschalten

```
gateway_enable="YES"
```

NAT Dämon starten

```
natd_enable="YES"
natd_interface="ed0"
natd_flags=""
```

Fürs Trafficshaping muss eine Kernelvariable gelöscht werden:

```
sysctl net.inet.ip.fw.one_pass=0
```

Das Firewallscript. Hier werden unsere definierten Regeln eingerichtet.

```
# RC Firewall
# /etc/rc.firewall
#
# Load firewall rules from /etc/firewall.rules
/sbin/ipfw -q flush
/sbin/ipfw -q /etc/firewall.rules

# EOF
```

In /etc/natd.conf befindet sich die Konfigurationsdatei für den NAT Dämon natd.

```
#
# /etc/natd.conf

#NATD config
#####################################################################
# Use sockets
use_sockets yes

# Try to use the same ports
same_ports yes

# Only alter outgoing packets with unregistered IPs
unregistered_only yes

# Use interface ed0 for natd
interface ed0

# Dynamic IP
dynamic
```

Die Durchzugsfirewall

```
# Divert traffic through NAT and allow everything else
########################################################################
add 10000 divert natd all from any to any via ed0
add 10010 pass all from any to any
```

Die Firewall soll von aussen her abgedichtet werden.

Diese beiden Regeln machen erst einmal alles zu und loggen alles, was auf sie zutrifft.

```
add 09000 deny log tcp from any to any
add 09010 deny log udp from any to any
```

Es empfiehlt sich, dem syslogd beizubringen, für ipfw ein separates Logfile zu schreiben. Dies geschieht durch folgenden Eintrag in /etc/syslog.conf:

```
!ipfw
*.*                                                    /var/log/ipfw.log
```

Damit ist unsere Firewall nun dicht von innen und aussen. =:-)
Nur den Stecker zu ziehen wäre noch sicherer. Die Benutzbarkeit bleibt dabei leider etwas auf der Strecke.

Nun wollen wir die Firewall für Datenverkehr vom innen nach aussen (vom LAN ins Internet) öffnen.

```
add 00100 skipto 9999 tcp from any to any established

add 00600 skipto 9999 tcp from 192.168.1.0/24 to any
add 00610 skipto 9999 udp from 192.168.1.0/24 to any
add 00610 skipto 9999 udp from any to 192.168.1.0/24
add 00620 skipto 9999 udp from any to any in recv ed0
add 00620 skipto 9999 udp from any to any out xmit ed0
add 00630 skipto 9999 ip from any to any out via ed0

add 00640 skipto 9999 icmp from any to any

add 00300 allow ip from any to any via lo0
add 00310 allow ip from any to any via rl0
```

Ja, und nun machen wir noch ein paar Löcher, damit gewisse Services von aussen erreichbar sind. Remote-Login per SSH soll möglich sein, und ein Webserver soll angesurft werden können.

```
add 00110 skipto 9999 tcp from any to any 22 in setup   # Allow SSH
add 00120 skipto 9999 tcp from any to any 80 in setup   # Allow Web
```

Für DCC Versand müssen ein paar Ports von aussen erreichbar gemacht werden. Diese Ports muss man auch in seinem Client als Range angeben, da DCC sonst wild irgendwelche Ports benutzt.

```
add 00130 skipto 9999 tcp from any to any 50000-50020 in setup
```

Ein paar Worte zum Trafficshaping

Trafficshaping wird ebenfalls über ipfw gesteuert. Dazu müssen sogenannte pipes definiert werden.

Um z.B. die Leitung nicht mit Downloads vom Webserver zu füllen, können wir die Bandbreite auf 90kbit/s limitieren.

Es empfiehlt sich, pipes vor allen anderen Rules einzuführen.

```
Add 00010 pipe 1 tcp from any 80 to any out via ed0
pipe 1 config bw 90 kbit/s
```

Mein Firewallscript für den Hausgebrauch sieht so aus:

```
#
# RC Firewall
#
#####################################################################
# Interface declaration
# lo0   : loopback interface
# ed0   : uplink to Cablecom
# rl0   : local 100Mbit Ethernet (nassacker)

# only for testing, has to be disabled
#####################################################################
#add 00001 allow ip from any to any

add 00100 skipto 9999 tcp from any to any established
add 00110 skipto 9999 tcp from any to any 22 in setup   # Allow SSH
add 00120 skipto 9999 tcp from any to any 80 in setup   # Allow Web
add 00130 skipto 9999 tcp from any to any 50000-50020 in setup
                                                        # Used for DCC


add 00300 allow ip from any to any via lo0
add 00310 allow ip from any to any via rl0



#####################################################################
```

```
# Reject private address space.
add 00500 deny log ip from 192.168.0.0/16 to 192.168.1.0/24 via ed0
add 00510 deny log ip from 192.168.1.0/24 to 192.168.0.0/16 via ed0
add 00520 deny log ip from 172.16.0.0/12 to any via ed0
add 00530 deny log ip from any to 172.16.0.0/12 via ed0
add 00540 deny log ip from 10.0.0.0/8 to any via ed0
add 00550 deny log ip from any to 10.0.0.0/8 via ed0

add 00600 skipto 9999 tcp from 192.168.1.0/24 to any
add 00610 skipto 9999 udp from 192.168.1.0/24 to any
add 00610 skipto 9999 udp from any to 192.168.1.0/24
add 00620 skipto 9999 udp from any to any in recv ed0
add 00620 skipto 9999 udp from any to any out xmit ed0
add 00630 skipto 9999 ip from any to any out via ed0
add 00640 skipto 9999 icmp from any to any

add 09000 deny log tcp from any to any
add 09010 deny log udp from any to any

# Divert traffic through NAT and allow everything else
#############################################################
add 10000 divert natd all from any to any via ed0
add 10010 pass all from any to any
```

Weiterführende Dokumentation zum Thema Firewalling und FreeBSD

- Manpages zu ipfw, natd und dummynet
- Das FreeBSD Handbook
  http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html
- Newsgroups
  de.comp.os.unix.bsd
  comp.unix.bsd.freebsd.misc