Installation

```
sudo apt-get fail2ban sendmail
```

Konfiguration

fail2ban wird mit einer Beispielkonfiguration geliefert. Diese befindet sich in der Datei `/etc/fail2ban/jail.conf`. Diese wird aber nicht für die Konfiguration von fail2ban verwendet. Dazu ist es nötig, dass die Datei in `jail.local` umbenannt / kopiert wird.

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Konfigurations-File für fail2ban ist unter /etc/fail2ban/fail2ban.conf zu finden

fail2ban.conf

```
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
#
# $Revision: 629 $
#

[Definition]

# Option:  loglevel
# Notes.:  Set the log level output.
#          1 = ERROR
#          2 = WARN
#          3 = INFO
#          4 = DEBUG
# Values:  NUM  Default:  3
#
loglevel = 3

# Option:  logtarget
# Notes.:  Set the log target. This could be a file, SYSLOG, STDERR or
STDOUT.
#          Only one log target can be specified.
# Values:  STDOUT STDERR SYSLOG file  Default:  /var/log/fail2ban.log
#
logtarget = /var/log/fail2ban.log

# Option: socket
# Notes.: Set the socket file. This is used to communicate with the
daemon. Do
```

```
# not remove this file when Fail2ban runs. It will not be
possible to
# communicate with the server afterwards.
# Values: FILE  Default:  /var/run/fail2ban/fail2ban.sock
#
socket = /var/run/fail2ban/fail2ban.sock
```

Nachfolgendes File ist für die einzelnen blockbaren Dienste:

/etc/fail2ban/jail.local

jail.local

```
# Fail2Ban configuration file.
#
# This file was composed for Debian systems from the original one
#  provided now under /usr/share/doc/fail2ban/examples/jail.conf
#  for additional examples.
#
# To avoid merges during upgrades DO NOT MODIFY THIS FILE
# and rather provide your changes in /etc/fail2ban/jail.local
#
# Author: Yaroslav O. Halchenko <debian@onerussian.com>
#
# $Revision: 281 $
#

# The DEFAULT allows a global definition of the options. They can be
override
# in each jail afterwards.

[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host
ignoreip = 127.0.0.1
bantime  = 86400
maxretry = 3

# "backend" specifies the backend used to get files modification.
Available
# options are "gamin", "polling" and "auto".
# yoh: For some reason Debian shipped python-gamin didn't work as
expected
#      This issue left ToDo, so polling is default backend for now
backend = polling

#
# Destination email address used solely for the interpolations in
# jail.{conf,local} configuration files.
destemail = patrick.schindelmann@googlemail.com
```

```
#
# ACTIONS
#

# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overriden globally or per
# section within jail.local file
banaction = iptables-multiport

# email action. Since 0.8.1 upstream fail2ban uses sendmail
# MTA for the mailing. Change mta configuration parameter to mail
# if you want to revert to conventional 'mail'.
mta = sendmail

# Default protocol
protocol = tcp

#
# Action shortcuts. To be used to define action parameter

# The simplest action to take: ban only
action_ = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s]

# ban & send an e-mail with whois report to the destemail.
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s]
            %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s",
protocol="%(protocol)s]

# ban & send an e-mail with whois report and relevant log lines
# to the destemail.
action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s",
protocol="%(protocol)s]
              %(mta)s-whois-lines[name=%(__name__)s,
dest="%(destemail)s", logpath=%(logpath)s]

# Choose default action.  To change, just override value of 'action'
with the
# interpolation to the chosen action shortcut (e.g.  action_mw,
action_mwl, etc) in jail.local
# globally (section [DEFAULT]) or per specific section
action = %(action_mwl)s

#
# JAILS
#

# Next jails corresponds to the standard configuration in Fail2ban 0.6
```

```
which
 # was shipped in Debian. Enable any defined here jail by including
 #
 # [SECTION_NAME]
 # enabled = true

 #
 # in /etc/fail2ban/jail.local.
 #
 # Optionally you may override any other parameter (e.g. banaction,
 # action, port, logpath, etc) in that section within jail.local

 [ssh]

 enabled = true
 port    = ssh
 filter = sshd
 logpath  = /var/log/auth.log
 maxretry = 4

 # Generic filter for pam. Has to be used with action which bans all
ports
 # such as iptables-allports, shorewall
 [pam-generic]

 enabled = false
 # pam-generic filter can be customized to monitor specific subset of
'tty's
 filter = pam-generic
 # port actually must be irrelevant but lets leave it all for some
possible uses
 port = all
 banaction = iptables-allports
 port     = anyport
 logpath  = /var/log/auth.log
 maxretry = 6

 [xinetd-fail]

 enabled   = false
 filter    = xinetd-fail
 port      = all
 banaction = iptables-multiport-log
 logpath   = /var/log/daemon.log
 maxretry  = 2

 [ssh-ddos]

 enabled = false
 port    = ssh
 filter  = sshd-ddos
```

```
logpath  = /var/log/auth.log
maxretry = 6

#
# HTTP servers
#

[apache]

enabled = false
port    = http,https
filter = apache-auth
logpath = /var/log/apache*/*error.log
maxretry = 6

# default action is now multiport, so apache-multiport jail was left
# for compatibility with previous (<0.7.6-2) releases
[apache-multiport]

enabled   = false
port     = http,https
filter   = apache-auth
logpath   = /var/log/apache*/*error.log
maxretry  = 6

[apache-noscript]

enabled = false
port    = http,https
filter  = apache-noscript
logpath = /var/log/apache*/*error.log
maxretry = 6

[apache-overflows]

enabled = false
port    = http,https
filter  = apache-overflows
logpath = /var/log/apache*/*error.log
maxretry = 2

#
# FTP servers
#

[vsftpd]

enabled  = true
port    = ftp,ftp-data,ftps,ftps-data
filter   = vsftpd
logpath  = /var/log/vsftpd.log
```

```
# or overwrite it in jails.local to be
# logpath = /var/log/auth.log
# if you want to rely on PAM failed login attempts
# vsftpd's failregex should match both of those formats
maxretry = 4


[proftpd]

enabled  = false
port    = ftp,ftp-data,ftps,ftps-data
filter   = proftpd
logpath  = /var/log/proftpd/proftpd.log
maxretry = 6


[wuftpd]

enabled  = false
port    = ftp,ftp-data,ftps,ftps-data
filter   = wuftpd
logpath  = /var/log/auth.log
maxretry = 6


#
# Mail servers
#

[postfix]

enabled  = false
port    = smtp,ssmtp
filter   = postfix
logpath  = /var/log/mail.log


[couriersmtp]

enabled  = false
port    = smtp,ssmtp
filter   = couriersmtp
logpath  = /var/log/mail.log


#
# Mail servers authenticators: might be used for smtp,ftp,imap
servers, so
# all relevant ports get banned
#
```

```
[courierauth]

enabled  = false
port    = smtp,ssmtp,imap2,imap3,imaps,pop3,pop3s
filter   = courierlogin
logpath  = /var/log/mail.log


[sasl]

enabled  = false
port    = smtp,ssmtp,imap2,imap3,imaps,pop3,pop3s
filter   = sasl
logpath  = /var/log/mail.log


# DNS Servers


# These jails block attacks against named (bind9). By default, logging
is off
# with bind9 installation. You will need something like this:
#
# logging {
#     channel security_file {
#         file "/var/log/named/security.log" versions 3 size 30m;
#         severity dynamic;
#         print-time yes;
#     };
#     category security {
#         security_file;
#     };
# }
#
# in your named.conf to provide proper logging

# Word of Caution:
# Given filter can lead to DoS attack against your DNS server
# since there is no way to assure that UDP packets come from the
# real source IP
[named-refused-udp]

enabled  = false
port     = domain,953
protocol = udp
filter   = named-refused
logpath  = /var/log/named/security.log

[named-refused-tcp]

enabled  = false
```

```
port     = domain,953
protocol = tcp
filter   = named-refused
logpath  = /var/log/named/security.log
```

In neueren Versionen von fail2ban werden die Apache2-Fehler „File not found“ in der Regel apache2-nohome abgearbeitet. Diese Regel ist bei bedarf noch einzufügen.

jail.conf

```
[apache-nohome]

enabled   = true
port      = http,https
filter    = apache-nohome
logpath   = /var/log/apache*/*error.log
maxretry  = 6
```

Server starten

```
sudo /etc/init.d/fail2ban start
```

Regeln testen

Wie testet man, ob eine Regel bei einer bestimmten Fehlermeldung greift? Dies kann man über das Tool fail2ban-regex prüfen. Der Syntax ist

```
fail2ban-regex [Option] <log> <regex> [ignoreregex]
```

Für <log> kann das Log-File angegeben werden (z.B. /var/log/apache2/error.log) oder ein String aus dieser Datei genommen werden. Genauso verhält es sich bei <regex>

Nach betätigen der Enter-Taste prüft das Tool, welche Fehlermeldung nach welcher Regel blockiert wird