????

- F.A.Q
- fail2ban 0.9.2 on Debian
- Fail2ban ?????
- ??iptables ? fail2ban ???
- ? WebServer-Apache ???
- ?? Embedded ????

- Fail2Ban ??????(???)
- How to protect your server with badIPs.com and report IPs with Fail2ban on Debian
- With OpenVZ Container
  - ? Just a note about iptables, fail2ban and NTPD to work.

?????www.fail2ban.org/wiki/index.php

???????https://github.com/fail2ban/fail2ban

????

for Ubuntu 16/18)

#> apt update
#> apt install fail2ban

????

#> fail2ban-client -h

for SuSE)

yast > Software > Software Management >

Search Phrase = fail2ban <Enter>

Actions = Install <???????>

Accept <Enter>

for CentOS)

?? EPEL ????
NOTE: ????????? epel-release-XX.noarch.rpm

wget http://mirror01.idc.hinet.net/EPEL/6/i386/epel-release-6-8.noarch.rpm
rpm -ivh epel-release-6-8.noarch.rpm
yum install fail2ban

??????

chkconfig --add fail2ban
chkconfig fail2ban on

????

#> fail2ban-client -h

?? Fail2ban
vi /etc/fail2ban/filter.d/asterisk.conf

```
# Fail2Ban configuration file
#
#
# $Revision: 250 $
#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
#before = common.conf


[Definition]

#_daemon = asterisk

# Option:  failregex
# Notes.:  regex to match the password failures messages in the logfile. The
#          host must be matched by a group named "host". The tag "<HOST>" can
#          be used for standard IP/hostname matching and is only an alias for
#          (?::f{4,6}:)?(?P<host>\S+)
# Values:  TEXT
#

failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - No matching peer found
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Username/auth name mismatch
            NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Device does not match ACL
            NOTICE.* .*: Registration from '.*" .* failed for '<HOST>' - Peer is not supposed to register
            NOTICE.* <HOST> failed to authenticate as '.*'$
            NOTICE.* .*: No registration for peer '.*' \(from <HOST>\)
            NOTICE.* .*: Host <HOST> failed MD5 authentication for '.*' (.*)


# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
```

ignoreregex =

vi /etc/fail2ban/jail.conf

```
# Important: exclude your local network in the ban IPs list
ignoreip = 127.0.0.1 192.168.0.0/16

## This is for SSH on OpenSUSE only.
## If enable, change 'false' as 'true'
[ssh-iptables]

enabled  = false
filter   = sshd
action   = iptables[name=SSH, port=ssh, protocol=tcp]
        sendmail-whois[name=SSH, dest=you@mail.com, sender=fail2ban@mail.com]
logpath  = /var/log/messages
maxretry = 5

##
[asterisk-iptables]

enabled  = true
filter   = asterisk
action   = iptables-allports[name=ASTERISK, protocol=all]
        sendmail-whois[name=ASTERISK, dest=root, sender=fail2ban@example.org]
logpath  = /var/log/asterisk/fail2ban
maxretry = 5
bantime = 259200
```

NOTES:

? logpath ???????? logger.conf ??????
? ???? ssh-iptables?????? fail2ban ?????? fail2ban.log ??????????????
fail2ban.actions.action: ERROR iptables -N fail2ban-SSH
iptables -A fail2ban-SSH -j RETURN
iptables -I INPUT -p tcp --dport ssh -j fail2ban-SSH returned 400
? ????? LAN ????? ignoreip??????????????

? ??? CentOS 5.x?[ssh-iptables]?????
logpath = /var/log/secure

?? Asterisk

??: 1.6.2.x
??/etc/asterisk/logger.conf

```
[general]
dateformat=%F %T

[logfiles]
console => notice,warning,error
messages => notice,warning,error,debug,verbose
fail2ban => notice
```

NOTES:

?? dateformat ? fail2ban logfile

??: 11.x

```
...
[logfiles]
...
fail2ban => notice,warning,security
```

Asterisk ?????

```
#> asterisk -rx "logger reload"
#> asterisk -rx "logger show channels"
```

?? Fail2ban

// ?? Asterisk ? logger ??

```
# asterisk -rx "module reload logger"
# asterisk -rx "logger show channels"

Channel                    Type    Status   Configuration
-------                   ----    ------   -------------
/var/log/asterisk/fail2ban        File    Enabled    - Notice
/var/log/asterisk/messages        File    Enabled    - Debug Verbose Warning Notice Error
                          Console  Enabled    - Warning Notice Error
```

// ???????? Fail2ban

yast > System

// ?????? Fail2ban

/etc/init.d/fail2ban start

// ?? iptables ??????

```
# iptables -L -nv

Chain INPUT (policy ACCEPT 5561K packets, 966M bytes)
 pkts bytes target     prot opt in     out     source               destination
  216 16120 fail2ban-SSH  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
23182 1973K fail2ban-ASTERISK  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 5091K packets, 884M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain fail2ban-ASTERISK (1 references)
 pkts bytes target     prot opt in     out     source               destination
23182 1973K RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain fail2ban-SSH (1 references)
 pkts bytes target     prot opt in     out     source               destination
   18  1788 DROP       all  --  *      *       123.123.123.123      0.0.0.0/0
  198 14332 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

NOTES:

fail2ban-SSH ????????? jail.conf ?? SSH-iptables ??????

???/?????(??)

???fail2ban ?????? IPs ??

?? 3 ???

- /etc/fail2ban/action.d/iptables-allports.conf
- /etc/fail2ban/action.d/iptables-multiport.conf
- /etc/fail2ban/action.d/iptables.conf

?????

```
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I <chain> -p <protocol> --dport <port> -j fail2ban-<name>
...
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
...
actionunban = iptables -D fail2ban-<name> -s <ip> -j DROP
```

?????

```
actionstart = ...
              ...
              ...
              for IP in `cat /etc/fail2ban/ip.deny`; do iptables -I fail2ban-<name> 1 -s $IP -j DROP;done
...
...
actionban = if [ -z `awk '$1 == "<ip>" { print "true" }' /etc/fail2ban/ip.allow` ] && [ -z `awk '$1 == "<ip>" {
print "true" }' /etc/fail2ban/ip.deny` ]; then iptables -I fail2ban-<name> 1 -s <ip> -j DROP;fi
...
...
actionunban = if [ -z `awk '$1 == "<ip>" { print "true" }' /etc/fail2ban/ip.allow` ] && [ -z `awk '$1 == "<ip>" {
print "true" }' /etc/fail2ban/ip.deny` ]; then iptables -D fail2ban-<name> -s <ip> -j DROP;fi
```

???????

1. /etc/fail2ban/ip.deny (???)
2. /etc/fail2ban/ip.allow (???)

???????????????? fail2ban ??????

F.A.Q

Q:????????

Ans: ????? log ?????????????????????

????? log ???

[2015-01-28 05:40:16] NOTICE[-1] Ext. 9015448702956577: Incoming SIP connection from unknown peer failed for 31.3.244.234 - Unknown connection from peer

? /etc/fail2ban/filter.d/asterisk.conf ???????

NOTICE.* .*: Incoming SIP connection from unknown peer failed for <HOST> - Unknown connection from peer

??????????????????

#> fail2ban-regex /var/log/asterisk/fail2ban "NOTICE.* .*: Incoming SIP connection from unknown peer failed for <HOST> - Unknown connection from peer"

TIPS:

fail2ban-regex <path/to/log> <failregex or /etc/fail2ban/filter.s/XXX.conf>

Q:???? /var/log/fail2ban.log

Ans: ?? /etc/fail2ban/fail2ban.conf

```
#logtarget = SYSLOG
logtarget = /var/log/fail2ban.log
```

?? fail2ban ??

Q:??????????

Ans: ????? fail2ban ????????????????????? IP ????????????? IP?fail2ban ??????????

Q:? Elastix/CentOS 5.3 ???? ban IP

?? fail2ban-client ????? log ??????????? ban IP

```
# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:           asterisk-iptables

# fail2ban-client status asterisk-iptables
|- filter
| |- File list:       /var/log/asterisk/fail2ban
| |- Currently failed: 0
| `- Total failed:     0
`- action
  |- Currently banned: 0
  | `- IP list:
  `- Total banned:     0
```

?????

?? /etc/asterisk/logger.conf

```
;syslog keyword : This special keyword logs to syslog facility
;????????
syslog.local0 => notice,warning,error
```

Reload Asterisk

Q:??? IP ???????

```
# iptables -D fail2ban-ASTERISK -s 123.123.123.123 -j DROP
?
# iptables -L fail2ban-ASTERISK -nv --line-number
Chain fail2ban-ASTERISK (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       all  --  *      *       134.213.134.172      0.0.0.0/0
2        0     0 DROP       all  --  *      *       46.105.127.222       0.0.0.0/0
3        0     0 DROP       all  --  *      *       116.255.152.101      0.0.0.0/0
4     1364  363K RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

iptables -D fail2ban-ASTERISK 2 ;??? 2 ??

Q:?????????? IP ? DDoS ?? Received incoming SIP connection...

CLI Log?

Received incoming SIP connection from unknown peer to 003333002972597886748"

NOTE:

- ??????? sip_general.conf ? allowguest=yes (by default)??????
- ??????? *Sending fake auth rejection for device 100<sip:100@123.123.123.123>* ????????????? **?? allowguest=no**???????????
  ????????????? allowguest=no???? Asterisk 11 ?????Log ??????????? IP??????? Fail2ban ???????????
  ?????????

Ans:

1. ?? /etc/asterisk/extensions.conf

```
[from-sip-external]
; ????????????
exten => _.,1,NoOp(Received incoming SIP connection from unknown peer to ${EXTEN})
exten => _.,n,Set(DID=${IF($["${EXTEN:1:2}"=""]?s:${EXTEN})})
exten => _.,n,Set(foo=${SIPCHANINFO(recvip)})
exten => _.,n,Log(NOTICE,Incoming SIP connection from unknown peer failed for ${foo} - Unknown
connection from peer)
exten => _.,n,Hangup
exten => h,1,Hangup
exten => i,1,Hangup
exten => t,1,Hangup
```

?????

```
asterisk -rx "dialplan reload"
```

2. ?? /etc/fail2ban/filter.d/asterisk.conf

```
...
failregex = NOTICE.* .*: Registration from '.*' failed for '<HOST>' - Wrong password
        ...
        ...
        NOTICE.* .*: Incoming SIP connection from unknown peer failed for <HOST> - Unknown connection
from peer
```

?????

```
service fail2ban restart
```

Q:???? Sending fake auth rejection ...
? Asterisk 1.11+)

> Failed to authenticate device 1005<sip:1005@123.123.123.123>;tag=2071f8ca

? Asterisk 1.8)

> Sending fake auth rejection for device 100<sip:100@123.123.123.123>;tag=99fdd5d7
>
> 123.123.123.123 is my external IP of PBX

Ans??? Asterisk ???????

Asterisk 11)
?????? Security Log Level ???????????????????? IP?????? fail2ban ????

?? /etc/fail2ban/filter.d/asterisk.conf
?? SECURITY ??

failregex = Registration from '.*' failed for '<HOST>:.*' - Wrong password
...
...
SECURITY.* .*:
SecurityEvent="(FailedACL|InvalidAccountID|ChallengeResponseFailed|InvalidPassword)",EventTV="[\d-]+",Severit

?????

1. http://highsecurity.blogspot.tw/2013...l2ban-088.html
2. http://issues.freepbx.org/browse/FREEPBX-7573

Asterisk 1.8/1.6)
??? Asterisk ?????????????? channels/chan_sip.c????????????? IP?????????? Asterisk ????????? fail2abn ??
??

?????https://bugs.debian.org/cgi-bin/bugr...cgi?bug=706739

TIP?

> ???? Asterisk ??????????? chan_sip.c ??????????????????

????

- Preventing Brute Force Attacks With Fail2ban On OpenSUSE 10.3
- Fail2ban - Asterisk

- Fail2Ban (with iptables) And Asterisk (voip-info)
- Install Fail2Ban on Elastix 1.6
- fail2ban and iptables (on-line PDF)
- http://centoshelp.org/security/fail2ban/
- http://net.nthu.edu.tw/2009/security:fail2ban
- Protect Asterisk with Fail2Ban on Debian 5
- Fail2ban Manual Unban Single Host (for iptables)