

Fail2Ban FAQ

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

```
“ WARNING Determined IP using DNS Lookup:
```

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

```
usedns = no
```

Q:[v0.10.0] ????????

```
“ iptables v1.4.14: unknown option "-w"
```

Ans????? iptables ???? v1.4.20 ??????????????????????

?? /etc/fail2ban/action.d/iptables-common.local

```
[Init]
lockingopt =
```

Q:[Asterisk] ?? Call Log ??????

```
“ Call from " (195.154.134.116:5071) to extension '8011441295298642'
  rejected because extension not found in context 'public'.
```

Ans??? Asterisk ? allowguest=no

?? sip.conf

```
allowguest=no
```

?????

```
#> asterisk -rx "sip reload"
#> asterisk -rx "sip show settings" | grep -i "Allow unknown access"
Allow unknown access: No
```

Q:[Asterisk] ??????????

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:[Asterisk] ? 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:[Asterisk] ?????????? IP ? DDoS ?? Received incoming SIP connection

“ CLI Log?

Received incoming SIP connection from unknown peer to 003333002972597886748"

??????? 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: ?? /etc/asterisk/extensions.conf

```
[from-sip-external]
; [REDACTED]
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
```

?? /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
```

Q:[Asterisk] ????? 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

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-
]+",Severity="[w]+",Service="[w]+",EventVersion="\d+",AccountID="\d+",SessionID="0x[\da-
f]+",LocalAddress="IPV[46]/(UD|TC)P/[\da-fA-
F:.]+\d+",RemoteAddress="IPV[46]/(UD|TC)P/<HOST>/\d+"(,Challenge="[w]+",ReceivedChallenge="[w+")]?(,Re
ceivedHash="[\da-f]+")?$
```

Asterisk 1.8/1.6)

??? Asterisk ?????????????????? channels/chan_sip.c????????????????? IP??????????????

Asterisk ?????????? fail2abn ????

Revision #2

Created 9 April 2021 03:52:59 by Admin

Updated 9 April 2021 08:57:32 by Admin