CARNET

Fail2Ban

CERT.hr-PUBDOC-2019-12-391

CERT.hr

Sadržaj

1 Uvod

Ispravno konfiguriran vatrozid (engl. *firewall*) jedna je od ključnih komponenti svakog sigurnog računalnog sustava. Nažalost, nije moguće unaprijed znati od kuda će dolaziti sav zlonamjeran promet i unaprijed ga blokirati. Zato sistemski administratori redovito (dnevno) čitaju i provjeravaju dnevnike (engl. *logs*) svojih sustava i sukladno zaključcima prilagođavaju postavke vatrozida.

Fail2Ban je softverski dodatak vatrozidu koji omogućuje automatsku detekciju i izolaciju određenih napada na sustav. Fail2Ban, jednako kao što to rade i sistemski administratori, čita dnevnike na poslužitelju te nakon određenog broja „ilegalnih“, tj. zlonamjernih radnji prilagođava pravila vatrozida kako bi izolirao i spriječio napadača od daljnjeg napada.

Vrlo često viđen napad na poslužitelje je uzastopno isprobavanje raznih lozinki u nadi da će se eventualno pogoditi ispravna (engl. *brute-force attack*). Fail2Ban jednostavnim pravilima može otežati, a u konačnici i zaustaviti takav napad, primjerice:

- Napadač isprobava razne lozinke, tj. izvršava *brute-force* napad, a svaki se pokušaj zabilježi u dnevniku.
- Fail2Ban čita dnevnike i, ako primijeti da je određena IP adresa u zadnjih nekoliko minuta više puta pogriješila lozinku, prilagođava pravila vatrozida na način da blokira napadačevoj IP adresi pristup sustavu na neko vrijeme (npr. 10 min).
- Napadač više ne može tako efikasno pogađati lozinke jer nakon određenog broja pokušaja mora čekati vrijeme koje definira Fail2Ban. Time je otežan *brute-force* napad. Fail2Ban može blokirati napadačevu IP adresu i na duže vrijeme, čime je *brute-force* napad s te IP adrese zaustavljen.

Također, alat Fail2Ban može jednostavno zaustaviti i drugi često viđen napad, a to je napad uskraćivanjem resursa (*engl. Denial-of-Service, DOS*). Ako se Fail2Ban postavi na način da spriječi pristup IP adresama koje troše previše resursa, može im onemogućiti pristup na određeno vrijeme čime sprječava DOS napad.

Fail2Ban je razvijen za POSIX sustave te je zbog svoje popularnosti dostupan u glavnim repozitorijima većine Linux distribucija.

2 Instalacija alata Fail2Ban

Službeni paketi za Fail2Ban su dostupni u većini Linux distribucija te je preporučeno putem njih instalirati alat. U nastavku su navedene naredbe za instalaciju na nekoliko popularnijih distribucija.

Naredbe je potrebno izvršiti s administratorskim privilegijama dodavanjem ključne riječi. `sudo` ispred svake naredbe:

Debian & Ubuntu

1. Najprije ažuriramo sustav:

   ```
   $ apt-get update

   $ apt-get upgrade
   ```

2. Instalacija alata Fail2Ban:

   ```
   $ apt-get install fail2ban
   ```

3. Pokretanje alata Fail2Ban:

   ```
   $ systemctl start fail2ban

   $ systemctl enable fail2ban
   ```

```
korisnik@debian:~$ sudo apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify python3-systemd whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify python3-systemd whois
0 upgraded, 4 newly installed, 0 to remove and 1 not upgraded.
Need to get 527 kB of archives.
After this operation, 2,560 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian buster/main amd64 fail2ban all 0.10.2-2.1 [38
5 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 python3-pyinotify all 0.9.6
-1 [26.9 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 python3-systemd amd64 234-2
+b1 [37.2 kB]
Get:4 http://deb.debian.org/debian buster/main amd64 whois amd64 5.4.3 [77.8 kB]
Fetched 527 kB in 0s (5,748 kB/s)
Selecting previously unselected package fail2ban.
(Reading database ... 26960 files and directories currently installed.)
Preparing to unpack .../fail2ban_0.10.2-2.1_all.deb ...
Unpacking fail2ban (0.10.2-2.1) ...
```

Slika 1 ***Instalacija alata Fail2Ban iz službenog repozitorija***

Fedora

1. Ažuriranje sustava:

```
$ dnf update
```

2. Instalacija alata Fail2Ban:

```
$ dnf install fail2ban
```

3. Pokretanje alata Fail2Ban:

```
$ systemctl start fail2ban
```

```
$ systemctl enable fail2ban
```

CentOS & RHEL

1. Ažuriranje sustava i instalacija EPEL repozitorija:

```
$ yum update
```

```
$ yum install epel-release
```

2. Instalacija alata Fail2Ban:

```
$ yum install fail2ban
```

3. Pokretanje alata Fail2Ban:

```
$ systemctl start fail2ban
```

```
$ systemctl enable fail2ban
```

Ako distribucija nema službeni paket za instalaciju alata Fail2Ban, instrukcije za ručnu instalaciju su dostupne u repozitoriju alata.

Gore navedene instrukcije pisane su za Fail2Ban inačicu v0.10.2 i operacijski sustav Debian 10 (Buster). Postupak instalacije vrlo je sličan i za ostale operacijske sustave.

Ako se instalacija uspješno izvršila, naredbom `fail2ban-client -version` će se ispisati trenutno instalirana inačica alata Fail2Ban. Kao što je već rečeno, u ovom slučaju je to Fail2Ban v0.10.2.

```
korisnik@debian:~$ fail2ban-client --version
Fail2Ban v0.10.2

Copyright (c) 2004-2008 Cyril Jaquier, 2008- Fail2Ban Contributors
Copyright of modifications held by their respective authors.
Licensed under the GNU General Public License v2 (GPL).
korisnik@debian:~$
```

Slika 2 ***Naredba za prikaz instalirane inačica alata Fail2Ban***

3 Korištenje alata Fail2Ban

3.1 Konfiguracija datoteke fail2ban.local

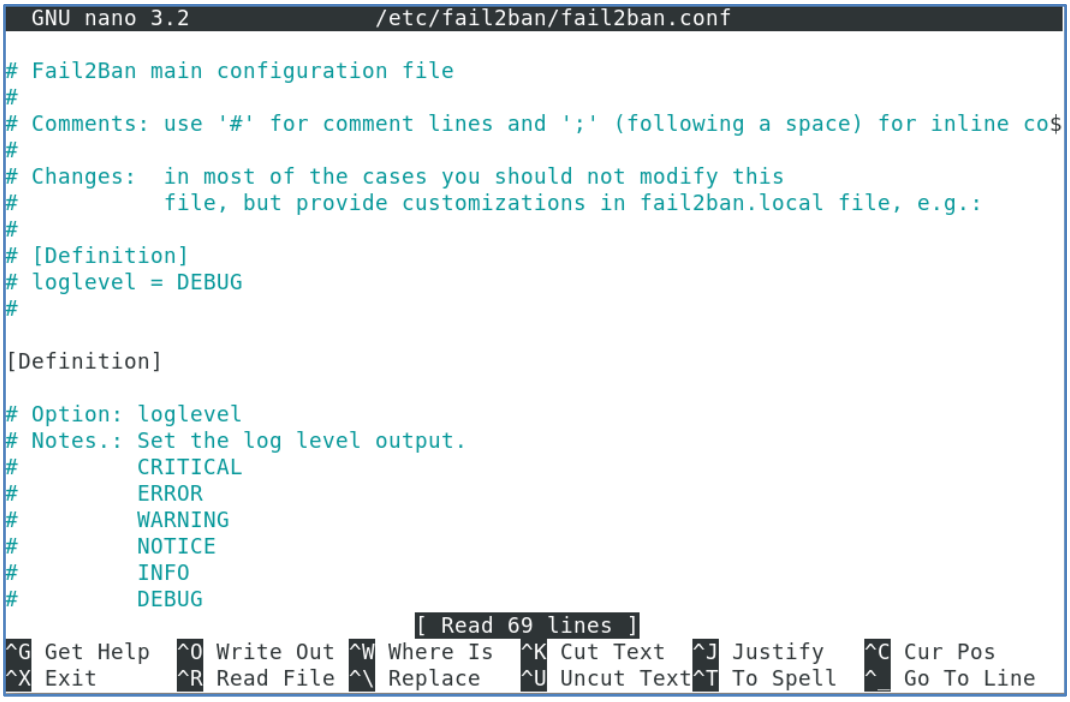
Nakon uspješne instalacije alata Fail2Ban, mogu se uređivati postavke. Sve svoje operacijske postavke Fail2Ban čita iz datoteke `fail2ban.conf` koja se nalazi u mapi `/etc/fail2ban/`. Preporučeno je ne mijenjati tu datoteku, nego stvoriti kopiju `fail2ban.local`. Jedan od načina za stvaranje kopije je korištenje naredbe:

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

Ako postoji datoteka `fail2ban.local`, Fail2Ban će čitati postavke iz te datoteke umjesto iz `fail2ban.conf`.

Tu datoteku je moguće mijenjati bilo kojim uređivačem teksta, npr. Nano:

```
$ nano /etc/fail2ban/fail2ban.local
```



Slika 3 Uređivanje datoteke fail2ban.local u uređivaču teksta Nano

Postavke koje se mogu uređivati su:

- `loglevel` – razina zapisa u dnevnik (CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG)
- `logtarget` – lokacija u koju se zapisuju događaji (datoteka, standardni izlaz…)
- `socket` – datoteka koja se koristi za komunikaciju s Fail2Ban poslužiteljem
- `pidfile` – datoteka gdje Fail2Ban sprema svoj identifikacijski broj procesa (PID)

- `dbfile` – datoteka gdje Fail2Ban trajno sprema podatke
- `dbpurgeage` – koliko često (u sekundama) Fail2Ban poništava zabrane zapisane u bazi podataka

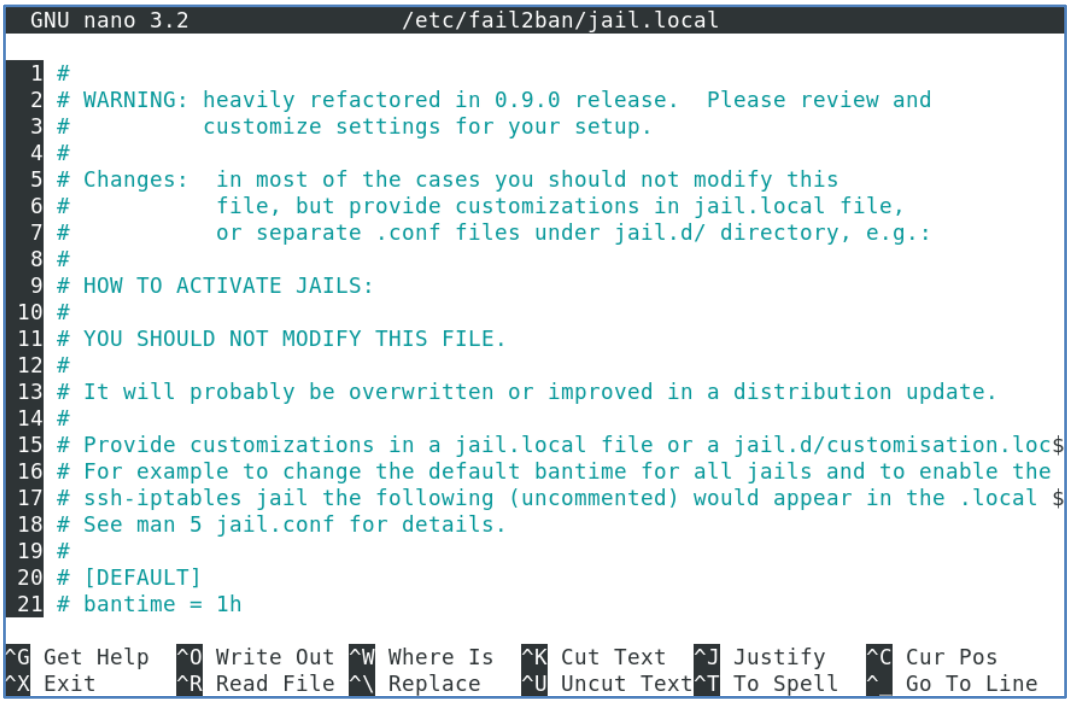
3.2 Konfiguracija zatvora (*engl. jail*)

Zanimljivije postavke, koje opisuju kako se točno štiti sustav, mogu se pronaći u datoteci `/etc/fail2ban/jail.conf`. Fail2Ban koristi takozvane zatvore (engl. *jail*) te u njima opisuje pravila po kojima će 'kažnjavati' aktivnosti koje se smatraju zlonamjernima. Ponovno je preporučeno ne mijenjati izravno izvornu datoteku, već stvoriti kopiju naredbom:

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

Nakon stvaranja, kopija se može uređivati nekim uređivačem teksta, npr. Nano:

```
$ nano /etc/fail2ban/jail.local
```



Slika 4 *Uređivanje datoteke jail.local u uređivaču teksta Nano*

Ovdje je moguće uređivati postavke poput:

- `ignoreip` – ip adresa kojoj nikad neće bit zabranjen pristup,
- `bantime` – koliko dugo će biti zabranjen pristup,
- `findtime` – koliko dugo će se pamtiti pokušaji pristupa,
- `maxretry` – koliko neuspjelih pokušaja se tolerira prije zabrane pristupa,

- `banaction` – radnja koja će se izvesti kad se prekrše gore navedena pravila,
- `protocol` – tip prometa koji će se zabraniti.

Bez komentara, tj. redova koji počinju znakom „#“, početak datoteke izgledao bi otprilike:

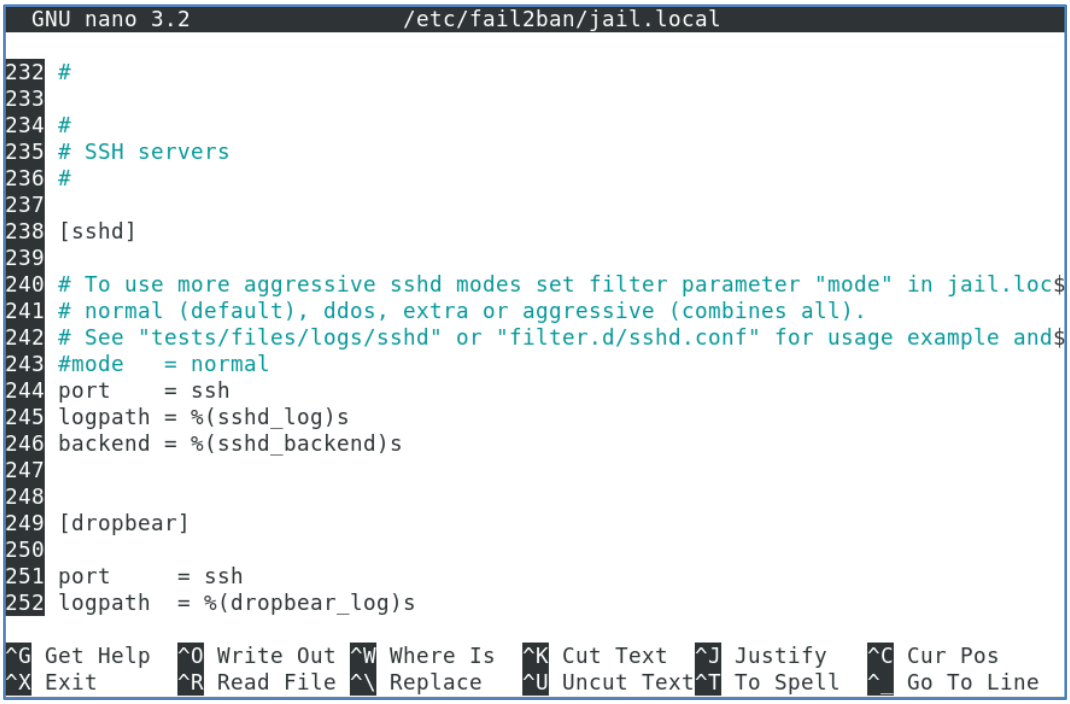
```
[DEFAULT]

ignoreip = 127.0.0.1/8

bantime = 600

findtime = 600

maxretry = 3

...
```

Ovo su izvorne postavke i mogu se prilagoditi za pojedine poslužitelje koji su pokrenuti na sustavu. Pojedini poslužitelji razlikuju se nazivom koji izgleda kao `[naziv_poslužitelja]`. Svaki poslužitelj trebao bi imati dvije postavke:

- `port` – priključak (engl. *port*) kojeg koristi poslužitelj
- `logpath` – dnevnik kojega fail2ban čita u slučaju neuspjelih pokušaja

Fail2Ban će većinu postavki preuzeti iz konfiguracija samih poslužitelja i zbog tog razloga tu nema potrebe za nekim većim izmjenama. Ako određena usluga (engl. *service*) treba imati neku postavku koja se razlikuje od izvorne, postavku treba promijeniti pod nazivom usluge (engl. *service*).

Primjer često prisutnog poslužitelja je SSH poslužitelj. Većina sustava koristi *sshd* (OpenSSH) pa se postavke mogu pronaći ispod naziva `[sshd]`.



Slika 5 ***Uređivanje pravila za poslužitelj sshd***

3.3 Konfiguracija filtera

Filteri određuju kriterije po kojima će zapisi u dnevnicima (engl. *log*) biti interpretirani kao neuspjeli pokušaj pristupa. Sve konfiguracije filtera se nalaze u direktoriju `/etc/fail2ban/filter.d/`.

Slika 6 ***Dostupni filteri unutar direktorija /etc/fail2ban/filter.d/***

Postavke filtera podijeljene su u dva dijela:

- `[INCLUDES]` – filteri koji su definirani u nekoj drugoj konfiguracijskoj datoteci, a primijenit će se zajedno s onima navedenima u trenutnoj konfiguracijskoj datoteci.
    - `before` – filteri koji će se primijeniti prije onih u trenutnoj datoteci
    - `after` – filteri koji će se primijeniti nakon onih u trenutnoj datoteci
- `[Definition]` – pravila filtriranja:
    - `failregex` – regularni izrazi (engl. *regex*) po kojima će se pretraživati dnevnik kako bi se pronašli zapisi koji odgovaraju neuspjelom pokušaju pristupa.
    - `ignoreregex` – Zapisi koji odgovaraju nekom od navedenih regularnih izraza (engl. *regex*) će se ignorirati. Npr. programi koji se nalaze na poslužitelju poput Systemd, CRON-a ili PostgreSQL-a generiraju velik broj zapisa i te zapise ćemo ignorirati.

Objašnjavanje pisanja regularnih izraza je izvan dosega ovog dokumenta, ali ukratko ćemo prokomentirati primjer u datoteci `counter-strike.conf` sa slike:

Slika 7 *Primjer filtriranja u konfiguracijskoj datoteci counter-strike.conf*

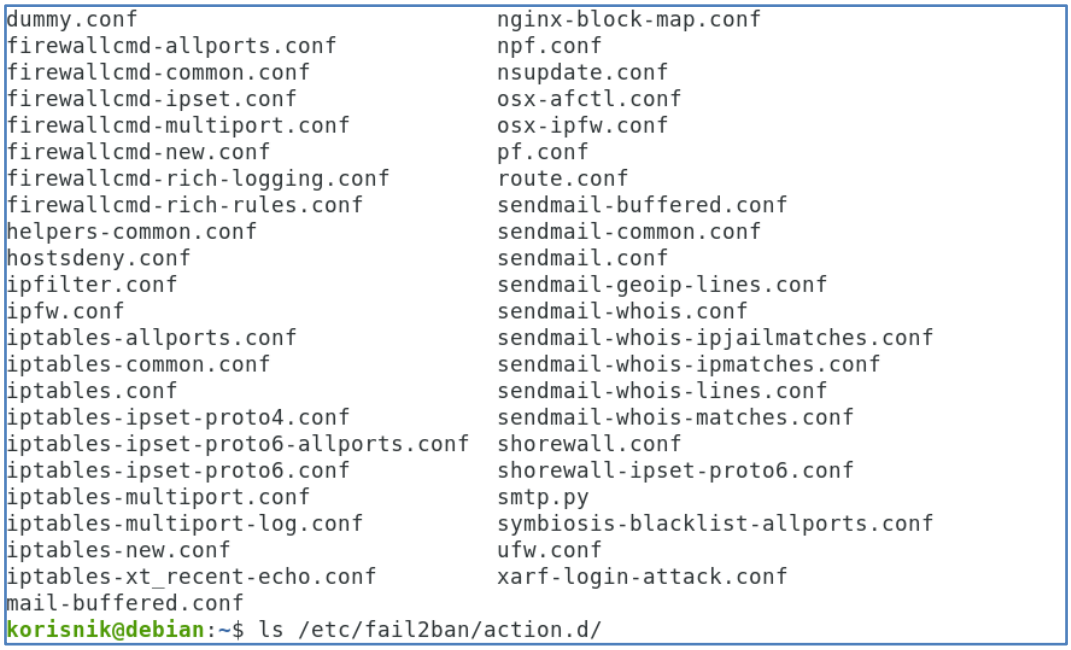
Dijela `[Include]` nema, što znači da se za filtriranje primjenjuju samo filteri navedeni u konfiguracijskoj datoteci `counter-strike.conf`.

Zapisi koje će poslužitelj zapisati u dnevnik, a u kojima se nalazi regularni izraz koji se sastoji od riječi „Bad Rcon“ (što označava pogrešno unesenu lozinku za udaljeni pristup konzoli) i podataka o klijentu koji je unio pogrešnu lozinku smatraju se neuspjelim

pokušajima pristupa, što ima smisla jer ako se netko više puta pokuša spojiti raznim pogrešnim lozinkama, vjerojatno je u tijeku *brute-force* napad.

3.4 Konfiguracija akcija

Zatvori opisuju pravila što je dopušteno, filteri opisuju kako će se detektirati zlonamjerne radnje, a akcije opisuju što će se dogoditi kada su pravila prekršena. Sve konfiguracije akcija se nalaze u `/etc/fail2ban/action.d/`.



Slika 8 *Dostupne akcije unutar direktorija /etc/fail2ban/action.d/.*

Akcije se sastoje od postavki podijeljenih u tri dijela:

- `[INCLUDES]` – akcije koje su definirane u nekoj drugoj konfiguracijskoj datoteci, a primijenit će se zajedno s akcijama definiranima u trenutnoj konfiguracijskoj datoteci:
    - `before` – akcije koje će se primijeniti prije onih u trenutnoj datoteci
    - `after` - akcije koje će se primijeniti nakon onih u trenutnoj datoteci
- `[Definition]` – definiranje akcija:
    - `actionstart` – radnja koja će se pokrenuti pokretanjem Fail2Bana.
    - `actionstop` – radnja koja će se pokrenuti gašenjem Fail2Bana.
    - `actioncheck` – radnja koja provjerava je li se sve ispravno pokrenulo.
    - `actionban` – radnja koja će se pokrenuti kršenjem pravila.
    - `actionunban` – radnja koja će se pokrenuti kad istekne „kazna“.

- [Init] – primjenjuje izvorne postavke u slučaju kad je akcija pozvana s manjkom parametra

Postavke poput `actionstart` su zapravo naredbe koje će sustav pokrenuti. Za primjer je preporučeno pogledati neke od već postojećih akcija poput `iptables-multiport.conf`.

```
  GNU nano 3.2     /etc/fail2ban/action.d/iptables-multiport.conf

# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> $
                           [ Read 52 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Slika 9 ***Primjer akcije definirane u konfiguracijskoj datoteci iptables-multiport.conf***

Među akcijama mogu se vidjeti akcije poput `sendmail`, koje se ne koriste za prilagođavanje vatrozida, već omogućuju slanje poruke e-pošte s obavijesti. Ova funkcionalnost iznimno je korisna sistemskim administratorima jer ih može obavijestiti o bitnim radnjama i upozoriti da provjere dnevnike i ustanove što se događa. Takve dodatne funkcionalnosti ne instaliraju se zajedno s Fail2Banom, već je za njihovo korištenje potrebno instalirati i konfigurirati dodatne pakete.

Fail2Ban se može prilagoditi na način da obavlja i druge, unaprijed definirane, radnje nakon što primijeti određene aktivnosti među zapisima u dnevniku, čime korisnici nisu ograničeni samo na dodavanje pravila u vatrozid.

4 Zaključak

Fail2Ban je jednostavan sustav zaštite koji prati dnevnike (engl. *logs*) i blokira napadača kad primijeti učestale radnje koje izgledaju kao da je riječ o mogućem napadu. Fail2Ban napadača blokira na način da blokira IP adrese s kojih dolaze napadi. Kako bi se provjerile IP adrese koje su blokirane može se unijeti naredba: `iptables -L`.

Fail2Ban nije jedini sustav zaštite temeljen na ovom principu, ali njegova prednost je jednostavnost i iz tog razloga je dobro prihvaćen među sistemskim administratorima. Fail2Ban kreće sa zaštitom sustava čim se instalira. Automatski štiti od SSH napada, iako je moguće zaštititi i druge servise.

Fail2Ban može gotovo u potpunosti eliminirati neke jednostavne napade koji se oslanjaju na uzastopno spajanje i slanje poruka mrežnim servisima. Uz to, Fail2Ban može otežati i vremenski usporiti i sofisticiranije napade ozbiljnijih napadača čime pomaže sigurnosnim stručnjacima i sistemskim administratorima da dobiju na vremenu i obrane se od raznih pokušaja napada.