Instalación de fail2ban para evitar ataques de fuerza bruta

Algunos enlaces:

https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-debian-7

https://www.upcloud.com/support/installing-fail2ban-on-debian-8-0/

https://www.fail2ban.org/wiki/index.php/MANUAL_0_8

http://xmodulo.com/how-to-protect-ssh-server-from-brute-force-attacks-using-fail2ban.html

Instalación:

```
apt install fail2ban
```

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

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

En Debian 12 da un problema al arrancarlo, cambiar en `/etc/fail2ban/jail.local`, en el apartado `[sshd]`

```
#mpf begin
#backend = %(sshd_backend)s
backend=systemd
enabled = true
#mpf end
```

El fichero `/etc/fail2ban/jail.local` (o `/etc/fail2ban/jail.conf`) permite configurarlo. Para alargar o acortar el tiempo que un host está bloqueado se utiliza el parámetro `bantime` indicando el tiempo en segundos.

```
bantime  = 1200
```

Después de modificar el fichero hay que reiniciar el servicio

```
/etc/init.d/fail2ban restart
```

Se pueden consultar las IPs bloqueadas con

```
fail2ban-client status sshd

Status for the jail: sshd
|- Filter
|  |- Currently failed: 2
|  |- Total failed:     12
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     2
```

```
   `- Banned IP list:   5.188.10.180
```

REJECT vs. DROP

Por defecto, las IPs bloqueadas reciben un REJECT `–reject-with icmp-port-unreachable`, para cambiarlo a DROP hay que editar el fichero `/etc/fail2ban/action.d/iptables-common.conf` y sustituir (o comentar) `blocktype`

```
blocktype = REJECT --reject-with icmp-port-unreachable
```

por

```
blocktype = DROP
```

https://gist.github.com/antoniocampos/1b8bc607d7b2d4a42e2a6e7df00645d0

No está muy claro si es mejor REJECT o DROP (sobre todo porque en este segundo caso lo usuarios legítimos se quedan bloqueados con un timeout muy grande), pero en el caso de ataques de fuerza bruta, creo que es mejor el DROP. https://unix.stackexchange.com/questions/109459/is-it-better-to-set-j-reject-or-j-drop-in-iptables y http://www.chiark.greenend.org.uk/~peterb/network/drop-vs-reject

Bloquear todos los puertos

Por defecto solo hace DROP del puerto ssh. Para bloquear todos los puertos hay que editar el fichero `/etc/fail2ban/jail.d/defaults-debian.conf` y añadir o modificar la siguiente entrada:

```
action = iptables[name=SSH, port="0:65535", protocol=tcp]
```

http://www.omniweb.com/wordpress/?p=1204

Bloquear el ping

Editar el fichero `/etc/fail2ban/action.d/iptables.conf` y añadir las siguientes entradas en `actionstart` y `actionstop`

```
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> --dport <port> -
j f2b-<name>
              <iptables> -I <chain> -p icmp -j f2b-<name>

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#
actionstop = <iptables> -D <chain> -p <protocol> --dport <port> -j
f2b-<name>
             <iptables> -D <chain> -p icmp -j f2b-<name>
             <iptables> -F f2b-<name>
```

```
            <iptables> -X f2b-<name>
```

https://www.digitalocean.com/community/tutorials/how-fail2ban-works-to-protect-services-on-a-linux-server

Bloquear y desbloquear IPs

Para desbloquear una IP

```
fail2ban-client set sshd unbanip 152.138.27.33
```

Para bloquear una IP

```
fail2ban-client set sshd banip 152.138.27.33
```

openvpn

Este parece que funciona:

https://peaksandprotocols.com/mitigating-an-openvpn-brute-force-attack-with-fail2ban-on-edgerouter/

Este de la web oficial es similar pero no «banea» (puede que sea tema de versiones):

https://www.fail2ban.org/wiki/index.php/HOWTO_fail2ban_with_OpenVPN

Otros que no he probado:

https://shankerbalan.net/blog/block-failed-openvpn-logins-with-fail2ban/
https://sourceforge.net/p/fail2ban/mailman/message/28865464/

Tracedump:

```
newBaseSize: 12pt
newBaseSizeInPt: 12
```