Fail2Ban support

Z-Push has a configuration option called `LOGAUTHFAIL`, by default set to `false` (disabled).

To enable it, set this configuration parameter to `true`.

This will cause an additional log entry in `WARN` level that will be logged to `z-push-error.log`.

The log message looks like this:

```
IP: 123.123.123.123 failed to authenticate user 'user@domain.com'
```

For a `systemd` server, use:

```
# FILE : /etc/fail2ban/filter.d/z-push.conf
# Fail2Ban configuration file
[INCLUDES]
before = common.conf
[Definition]
# 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>[\w\-.^_]+)
# Values:  TEXT
#
failregex = IP: <HOST> failed to authenticate user
ignoreregex =
[Init]
journalmatch = _SYSTEMD_UNIT=fail2ban.service
```

No `systemd` server, remove these two lines:

```
[Init]
journalmatch = _SYSTEMD_UNIT=fail2ban.service
```

If using `ufw` as firewall:

```
# UFW file /etc/fail2ban/action.d/ufw-all.conf
# Fail2Ban configuration file ufw-all.conf
#
# We add the rules to ufw for better control and management
#

[Definition]
actionstart =
actionstop =
actioncheck =
actionban = ufw insert 1 deny from <ip> to any
actionunban = ufw delete deny from <ip> to any
```

This is the actual configuration for `fail2ban`:

```
# Jail.local
[z-push]
enabled  = true
port     = http,https
filter   = z-push
banaction = ufw-all
# also enable define('LOGAUTHFAIL', true); in z-push/config.php or
/etc/z-push/z-push.conf.php
logpath  = /var/log/z-push/z-push-error.log
maxretry = 3
bantime  = 84600
```

The above configurations were contributed on 23.03.2016 by thctlo in the forum. Thanks!