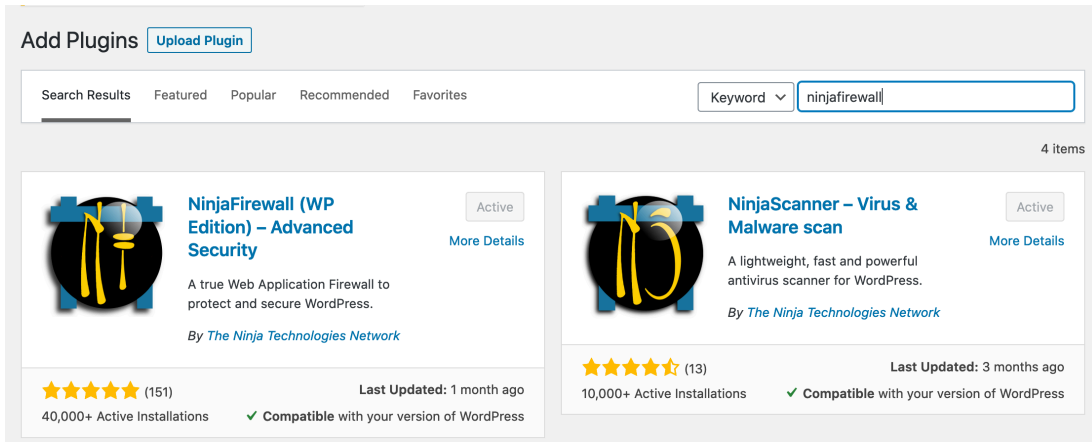
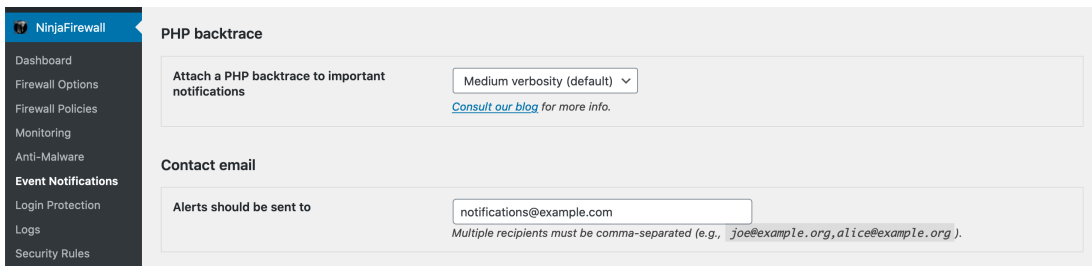


Step 1: install and activate NinjaFirewall

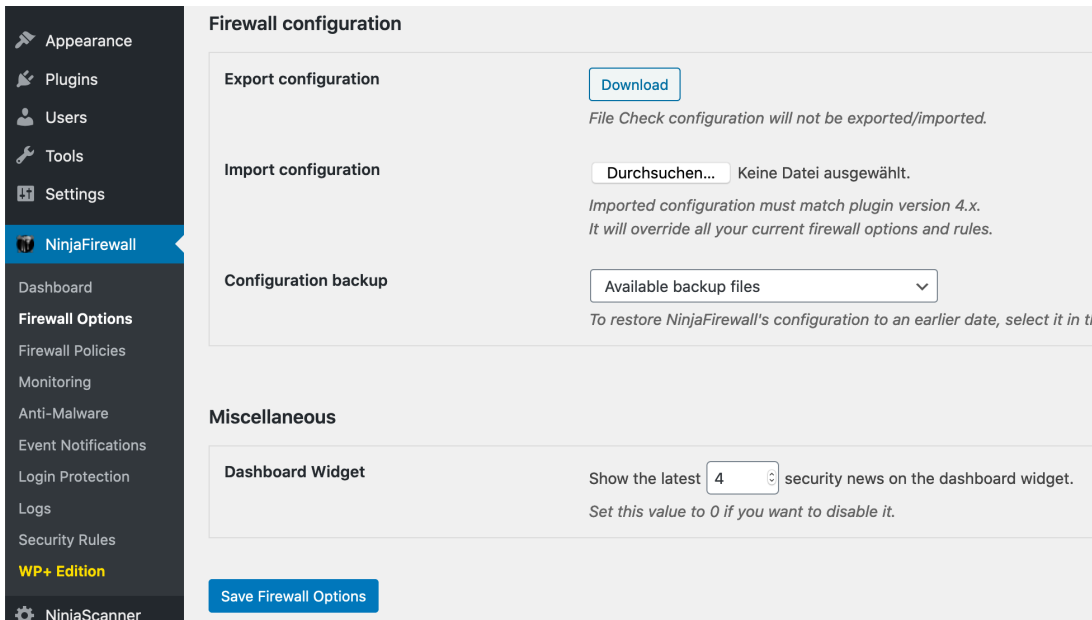


Step 2: go to NinjaFirewall – Event Notifications and copy the contact email

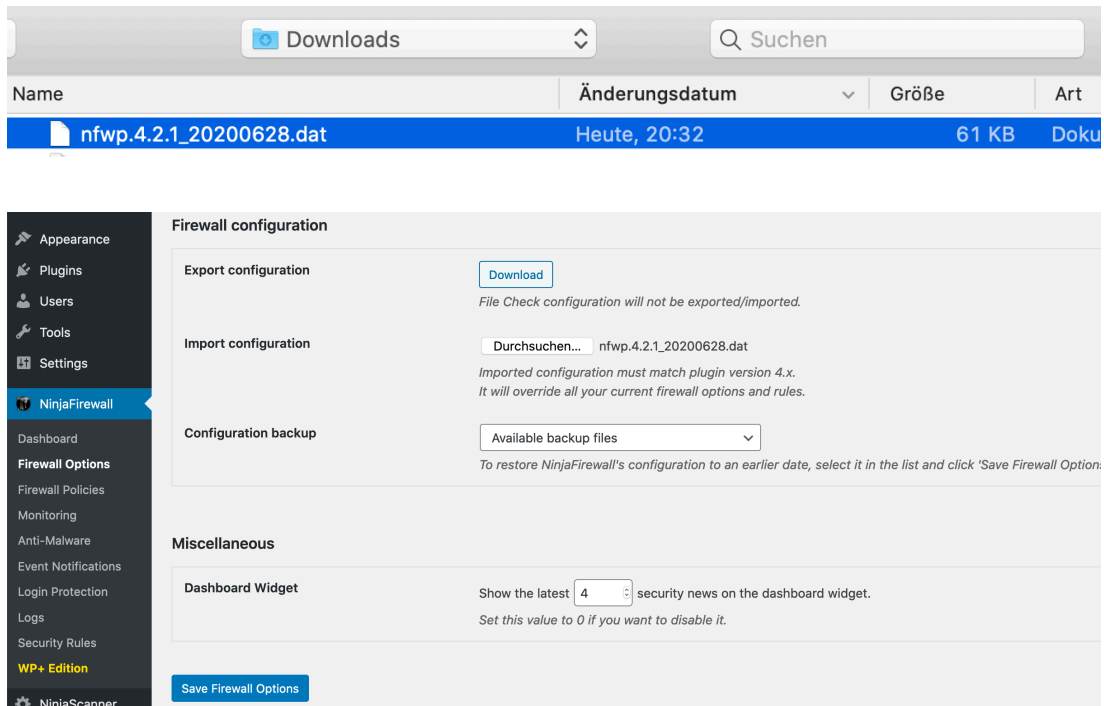


Step 3: go to <https://magos-securitas.com/downloads/> and download the configuration file

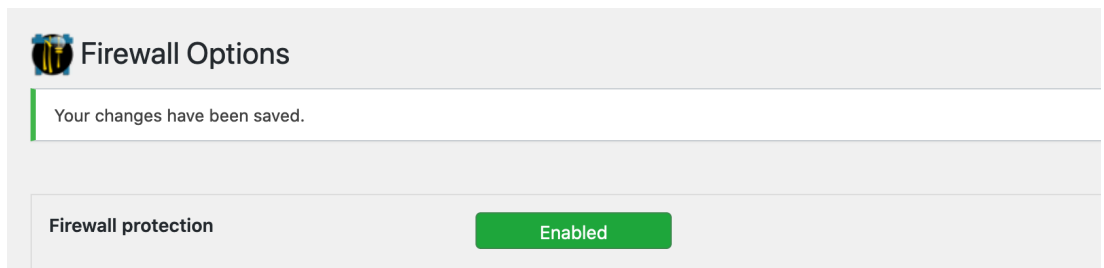
Step 4: go to NinjaFirewall – Firewall Options



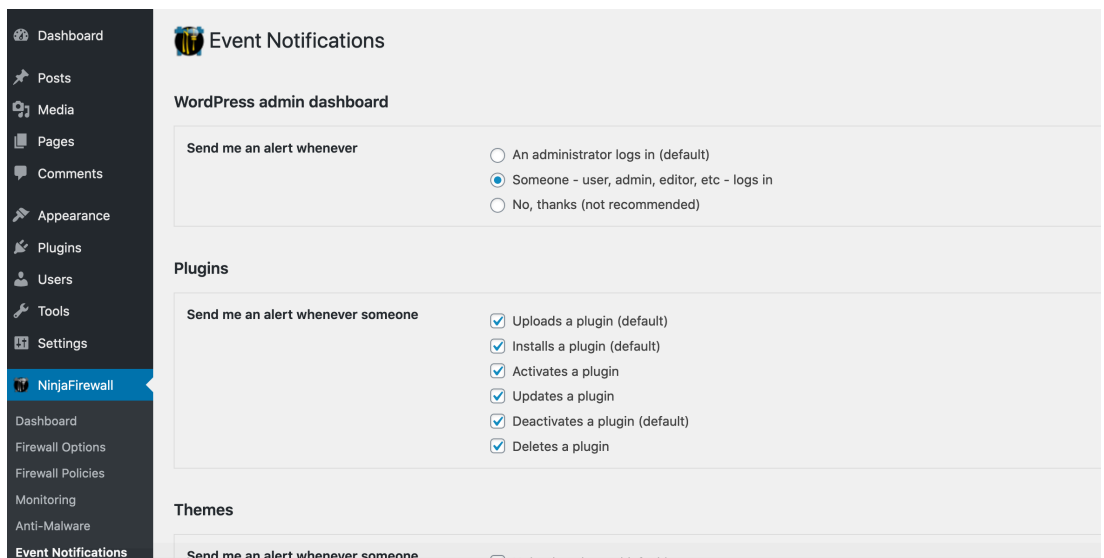
Step 5: import the downloaded configuration



Step 6: submit the page (in some cases you may have to repeat step 6 and 7)



Step 7: go to NinjaFirewall – Event Notifications, now all events should be enabled



Step 8: go to NinjaFirewall – Event Notifications and paste the contact email from step 2, save the form

The screenshot shows the 'Event Notifications' settings page. On the left is a sidebar menu with 'Event Notifications' selected. The main content area has two sections: 'PHP backtrace' and 'Contact email'. In the 'PHP backtrace' section, there is a dropdown menu set to 'Medium verbosity (default)' and a link to 'Consult our blog for more info.'. In the 'Contact email' section, there is a text input field containing 'notifications@example.com' and a note: 'Multiple recipients must be comma-separated (e.g., joe@example.org,alice@example.org)'.

Step 9: go to NinjaFirewall – Dashboard

The screenshot shows the 'Firewall Dashboard' page. The sidebar menu has 'Dashboard' selected. The main content area displays the following information:

Firewall	Enabled
Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, activate its Full WAF Activate Full WAF mode
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall
Version	4.3.1 ~ Security rules: 2021-01-27.2
PHP SAPI	FPM-FCGI ~ 7.3.25

Step 10: click on “Activate Full WAF mode”

[some very little tweaks](#). But in a few cases, mostly because of some shared hosting plans restrictions, it may simply not work at all. If this happened to you, don't worry: you could still run it in [WordPress WAF](#) mode. Despite being less powerful than the **Full WAF** mode, it offers a level of protection and performance much higher than other security plugins.

The screenshot shows the installation configuration page. It includes the following options:

- Select your HTTP server and your PHP server API (SAPI): Nginx + CGI/FastCGI or PHP-FPM (recommended) [dropdown menu]
- View [PHPINFO](#)
- Select the PHP initialization file supported by your server:
 - .user.ini (recommended)
 - php.ini
- Let NinjaFirewall make the necessary changes (recommended).
- I want to make the changes myself.
- Enable the sandbox.

If there were a problem during the installation, NinjaFirewall would undo those changes automatically for you.

[Finish Installation »](#)

Step 11: submit the page (scroll down to see the button, the default settings should be fine)

The screenshot shows a notification message from NinjaFirewall (WP Edition). The message reads: 'Oops! Full WAF mode is not enabled yet. Because PHP caches INI files, you may need to wait up to five minutes before the changes are reloaded by the PHP interpreter. Please wait for 291 seconds before trying again (you can navigate away from this page and come back in a few minutes)'. There is a close button (X) in the top right corner of the notification box.

Step 12: NinjaFirewall will create a .user.ini file next to the wp-config.php file

```
web >  .user.ini
1  ; BEGIN NinjaFirewall
2  auto_prepend_file = /var/www/html/web/app/nfwlog/ninjafirewall.php
3  ; END NinjaFirewall
4
5
```

Step 13: after some time the status should be updated (reload the page)

The screenshot shows the 'Firewall Dashboard' with a sidebar menu on the left containing 'Tools', 'Settings', 'NinjaFirewall', 'Dashboard', 'Firewall Options', 'Firewall Policies', 'Monitoring', and 'Anti-Malware'. The main content area displays the following information:

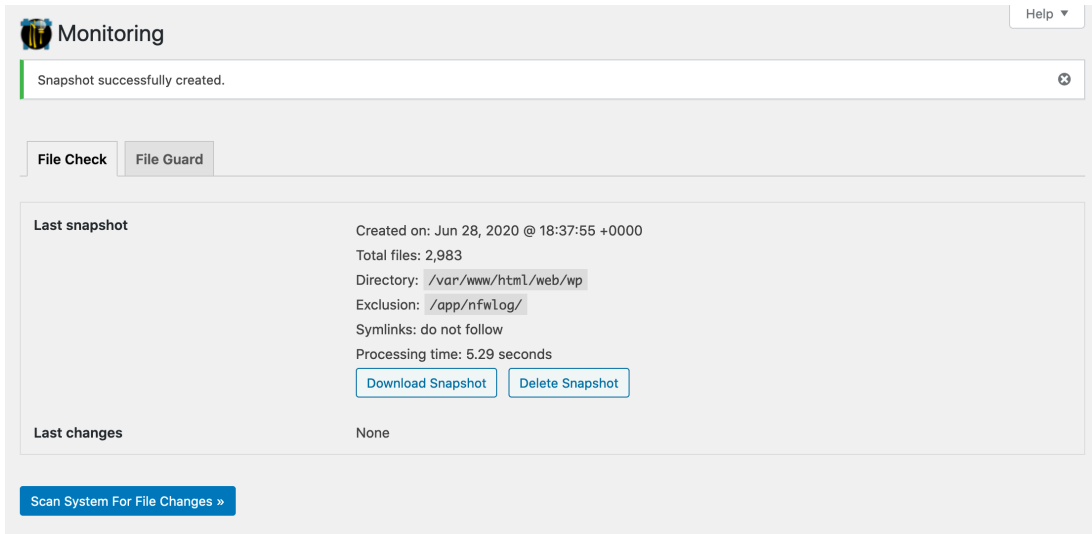
Firewall	Enabled
Mode	NinjaFirewall is running in Full WAF mode.
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall (WP+ Edition)
Version	4.2.1 ~ Security rules: 2020-06-26.1
PHP SAPI	FPM-FCGI ~ 7.3.15

Step 14: go to NinjaFirewall – Monitoring

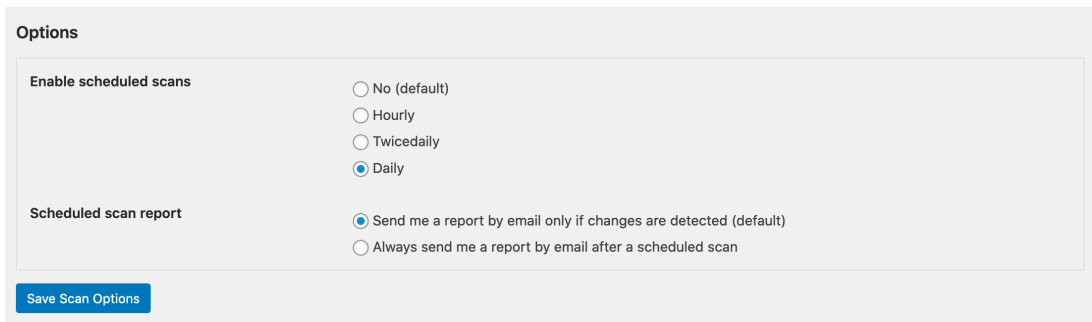
The screenshot shows the 'Monitoring' page with a sidebar menu on the left containing 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins', 'Users', 'Tools', 'Settings', 'NinjaFirewall', 'Dashboard', 'Firewall Options', 'Firewall Policies', 'Monitoring', and 'Anti-Malware'. The main content area has two tabs: 'File Check' (selected) and 'File Guard'. Below the tabs, there is a text box explaining: 'File Check lets you perform file integrity monitoring upon request or on a specific interval. To start, create a snapshot of your files by clicking the button below.' The settings form includes:

- 'Create a snapshot of all files stored in that directory' with a text input field containing '/var/www/html/web/wp/' and a default value of '/var/www/html/web/wp'.
- 'Exclude the following files/folders (optional)' with a text input field containing '/app/nfwlog/' and a note: 'Full or partial case-sensitive string(s). Multiple values must be comma-separated (,).'.
- A checked checkbox for 'Do not follow symbolic links (default)'.
- A 'Create Snapshot' button.

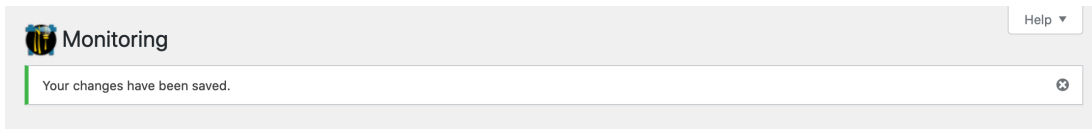
Step 15: create a snapshot



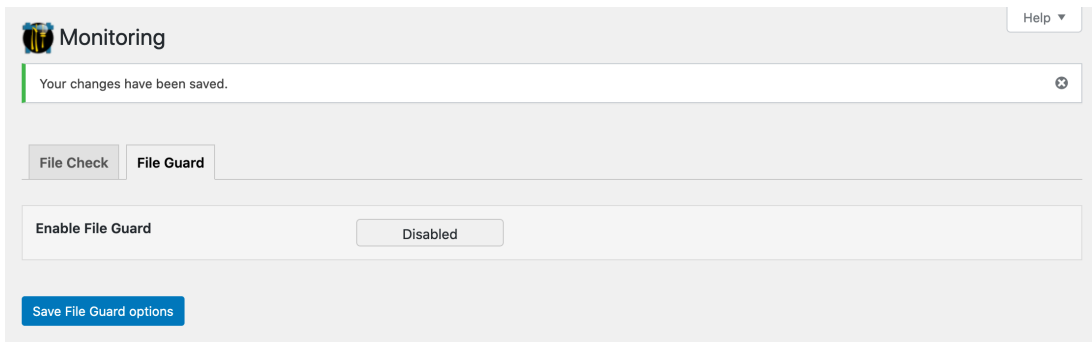
Step 16: set scan schedule to daily



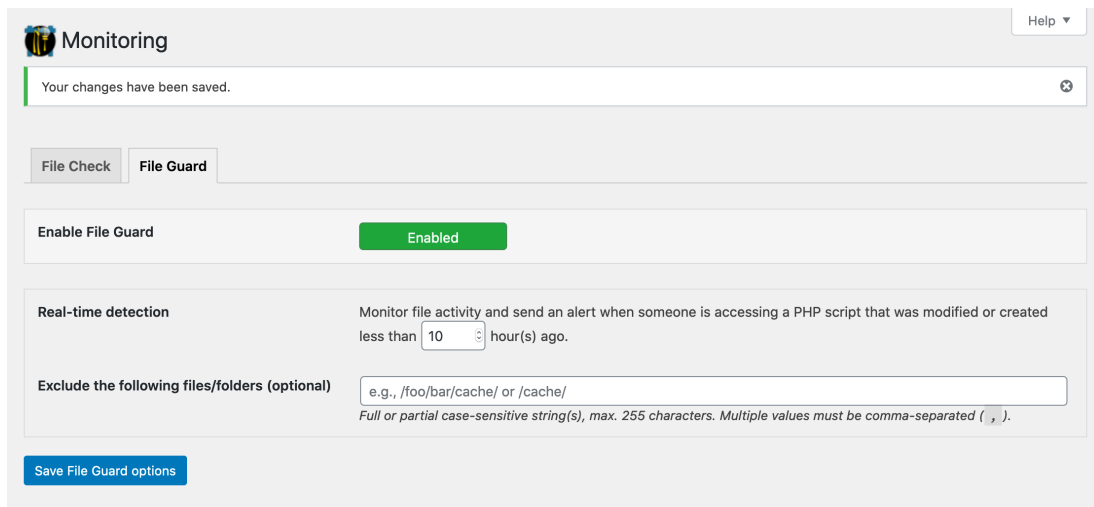
Step 17: click the save button



Step 18: go to File Guard on the same page



Step 19: enable File Guard and click the save button



Step 20: open a new incognito window and open `your-domain/wp-content/index.php?f=%00`, the request should be blocked and there should be the following information from NinjaFirewall which includes the event ID at the bottom



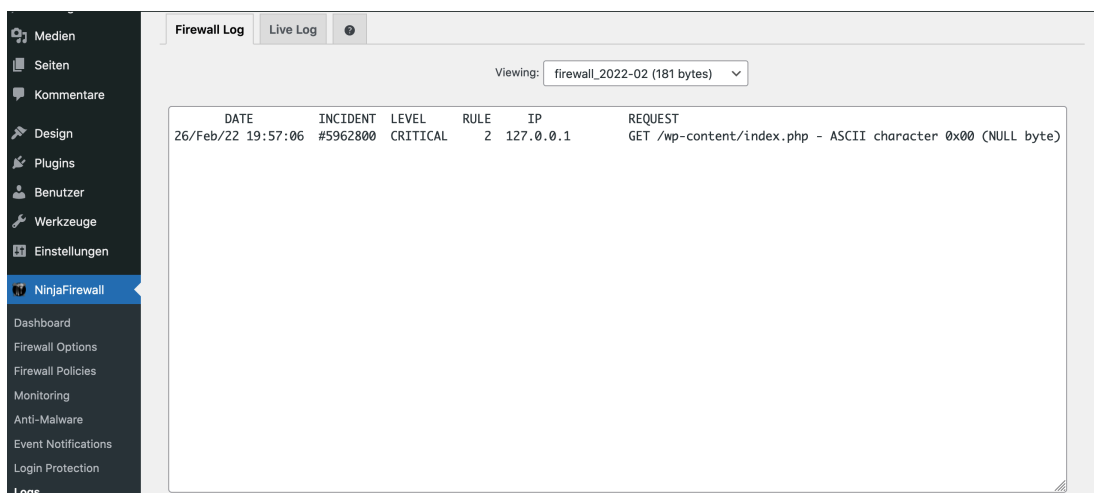
Sorry **127.0.0.1**, your request cannot be processed.
For security reasons, it was blocked and logged.



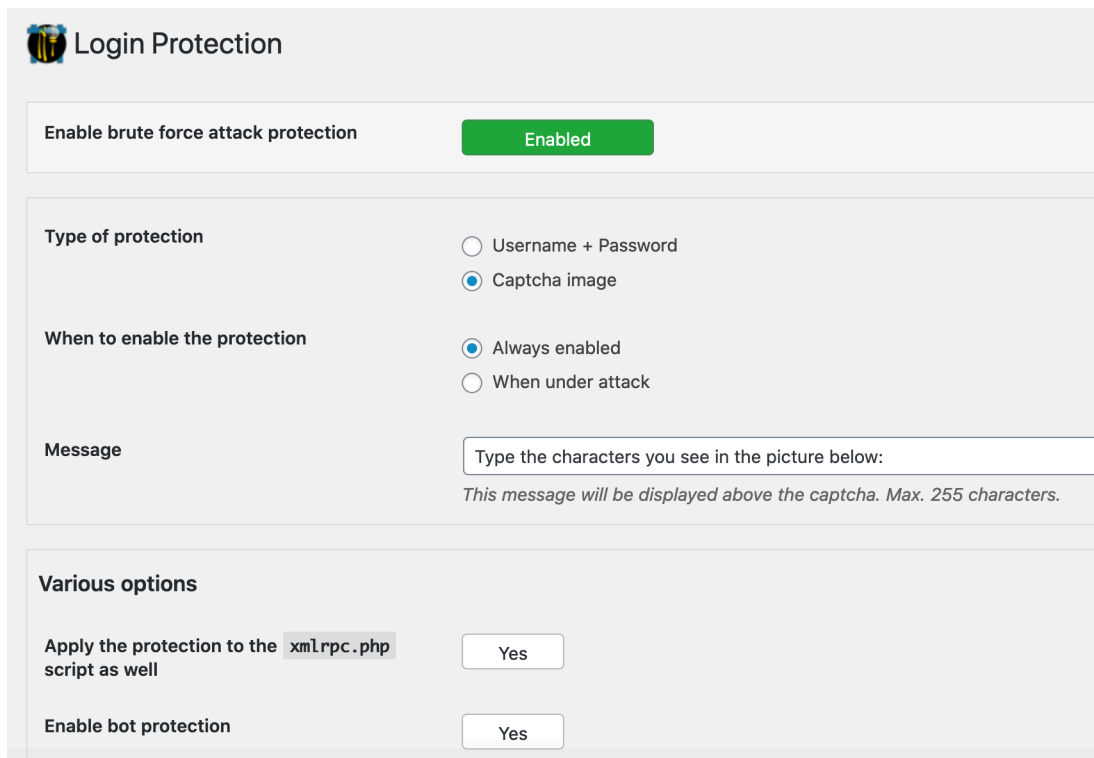
If you believe this was an error please contact the
webmaster and enclose the following incident ID:

[#5962800]

Step 21: go to NinjaFirewall – Logs, the blocked request should now appear there



Step 22 (optional): go to NinjaFirewall – Login Protection and use the following settings



The screenshot shows the 'Login Protection' configuration page. At the top left is a shield icon with a keyhole. The main title is 'Login Protection'. Below this, there are several sections:

- Enable brute force attack protection:** A green button labeled 'Enabled'.
- Type of protection:** Two radio button options: 'Username + Password' (unselected) and 'Captcha image' (selected).
- When to enable the protection:** Two radio button options: 'Always enabled' (selected) and 'When under attack' (unselected).
- Message:** A text input field containing 'Type the characters you see in the picture below:'. Below the field is a note: 'This message will be displayed above the captcha. Max. 255 characters.'
- Various options:** Two toggle buttons, both set to 'Yes':
 - 'Apply the protection to the `xmlrpc.php` script as well'
 - 'Enable bot protection'