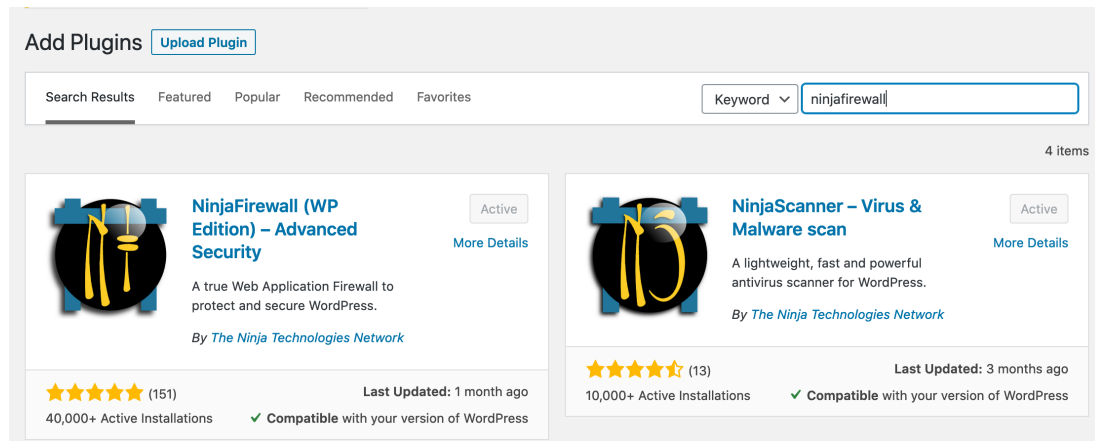


Schritt 1: installiere und aktiviere NinjaFirewall



Schritt 2: gehe zu NinjaFirewall – Event Notifications und kopiere die Kontakt-Emailadresse



Schritt 3: gehe zu [ninjafirewall config browser](#)

configuration file for NinjaFirewall WP Edition

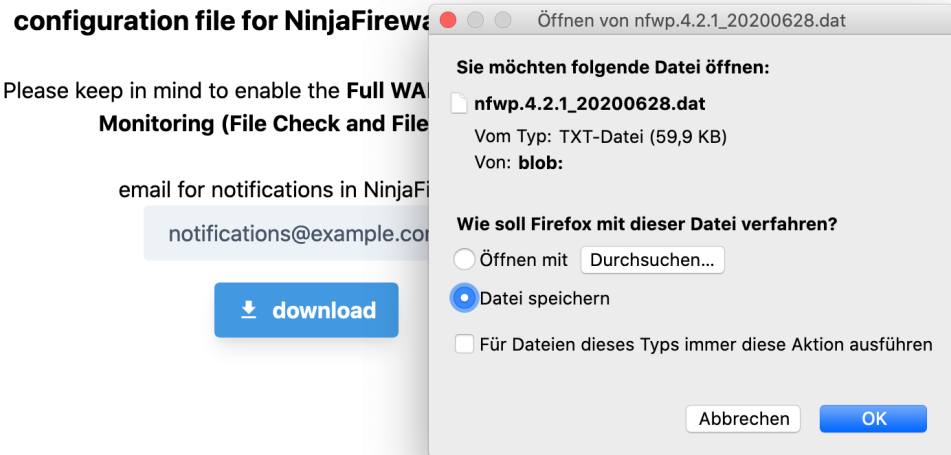
Please keep in mind to enable the **Full WAF Mode** and setup **Monitoring (File Check and File Guard)**.

email for notifications in NinjaFirewall:

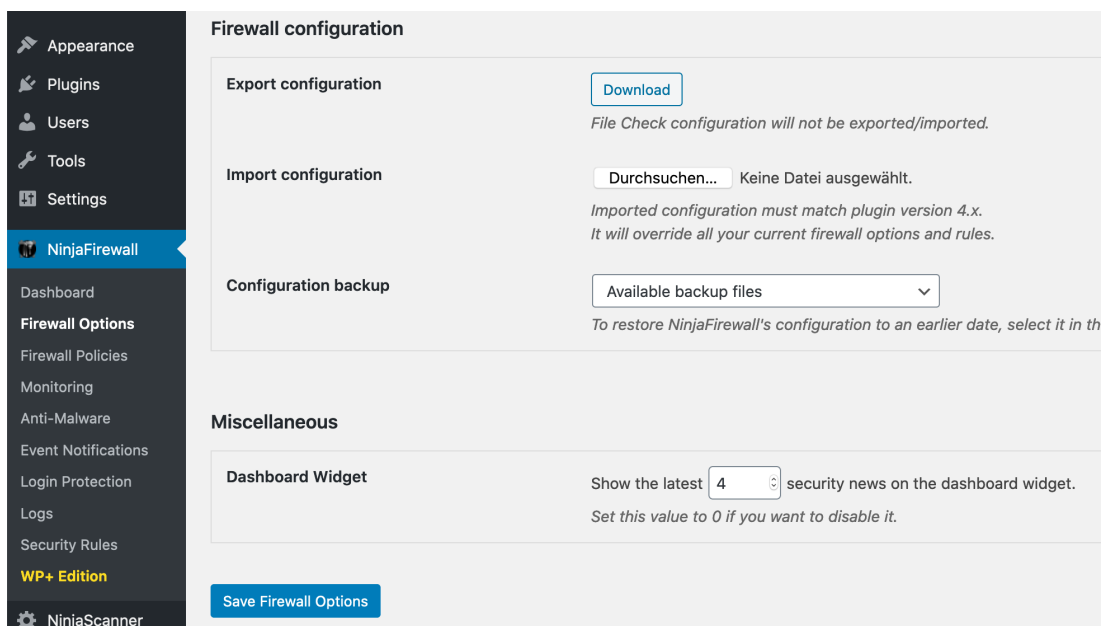
notifications@example.com

↓ download

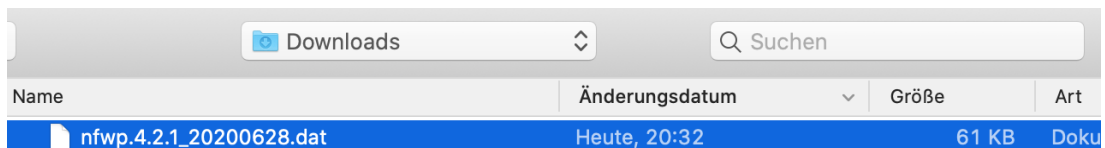
Schritt 4: füge die Kontakt-Emailadresse ein und klick den Download-Button



Schritt 5: gehe zu NinjaFirewall – Firewall Options



Schritt 6: importiere die heruntergeladene Konfigurations-Datei



Firewall configuration

Export configuration [Download](#)
File Check configuration will not be exported/imported.

Import configuration
Durchsuchen... nfwfp.4.2.1_20200628.dat
*Imported configuration must match plugin version 4.x.
It will override all your current firewall options and rules.*

Configuration backup
Available backup files
To restore NinjaFirewall's configuration to an earlier date, select it in the list and click 'Save Firewall Option'.

Miscellaneous

Dashboard Widget
Show the latest security news on the dashboard widget.
Set this value to 0 if you want to disable it.

[Save Firewall Options](#)

Schritt 7: speicher das Formular (in manchen Fällen müssen Schritt 6 und 7 wiederholt werden)

Firewall Options

Your changes have been saved.

Firewall protection [Enabled](#)

Schritt 8: gehe zu NinjaFirewall – Event Notifications, alle Events sollten angehakt sein

Event Notifications

WordPress admin dashboard

Send me an alert whenever
☐ An administrator logs in (default)
☒ Someone - user, admin, editor, etc - logs in
☐ No, thanks (not recommended)

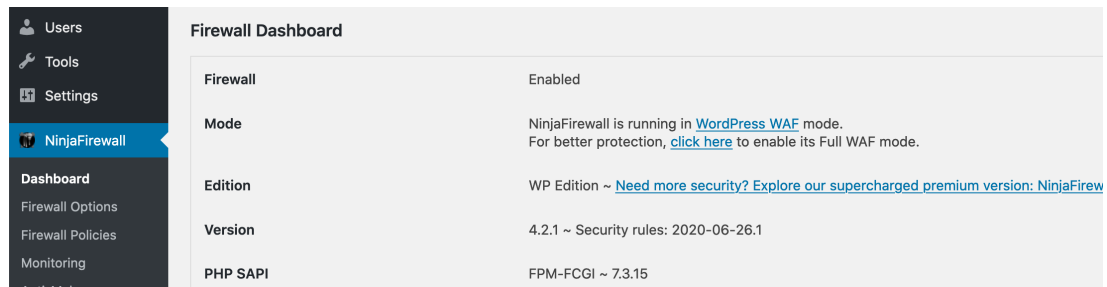
Plugins

Send me an alert whenever someone
☒ Uploads a plugin (default)
☒ Installs a plugin (default)
☒ Activates a plugin
☒ Updates a plugin
☒ Deactivates a plugin (default)
☒ Deletes a plugin

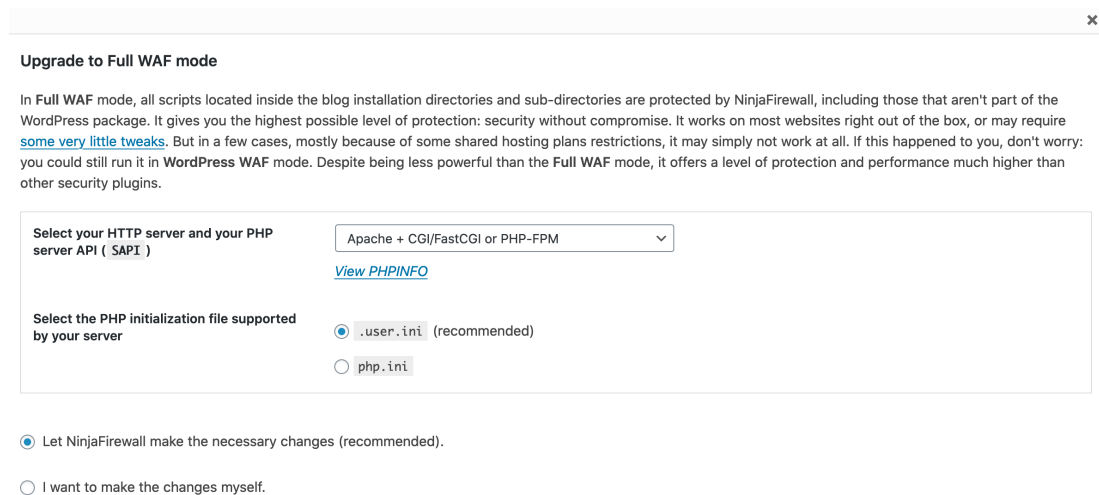
Themes

Send me an alert whenever someone
☒ Uploads a theme (default)

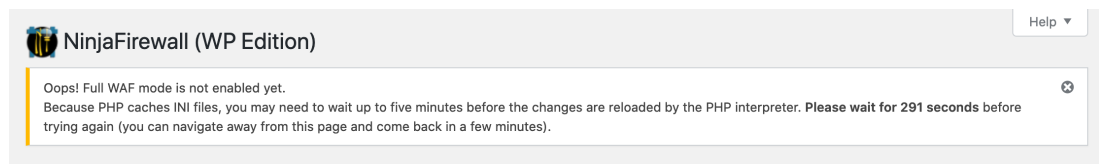
Schritt 9: gehe zu NinjaFirewall – Dashboard



Schritt 10: klick auf „click here“ um den Full WAF Modus einzurichten



Schritt 11: speicher das Formular (runterscrollen um den Button zu sehen, die ausgewählten Einstellungen sollten ok sein)



Schritt 12: NinjaFirewall wird eine .user.ini Datei auf der Ebene von wp-config.php erstellen

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

Schritt 13: nach ein paar Minuten sollte der Status aktualisiert sein (Seite neuladen)

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

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

Schritt 14: gehe zu NinjaFirewall – Monitoring

The screenshot shows the 'Monitoring' page with a sidebar 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 tabs for 'File Check' and 'File Guard'. Below the tabs, there is a text box explaining the File Check feature. Below that, there are input fields for 'Create a snapshot of all files stored in that directory' (with a default value of '/var/www/html/web/wp/') and 'Exclude the following files/folders (optional)' (with a value of '/app/nfwlog/'). There is also a checkbox for 'Do not follow symbolic links (default)' which is checked. A 'Create Snapshot' button is at the bottom.

Schritt 15: erstell einen Snapshot

The screenshot shows the 'Monitoring' page with a sidebar 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 tabs for 'File Check' and 'File Guard'. Below the tabs, there is a message 'Snapshot successfully created.' with a close button. Below that, there is a section for 'Last snapshot' with the following details:

Created on:	Jun 28, 2020 @ 18:37:55 +0000
Total files:	2,983
Directory:	/var/www/html/web/wp
Exclusion:	/app/nfwlog/
Symlinks:	do not follow
Processing time:	5.29 seconds

Below the details, there are buttons for 'Download Snapshot' and 'Delete Snapshot'. At the bottom, there is a section for 'Last changes' with the value 'None' and a button for 'Scan System For File Changes »'.

Schritt 16: setz das Scan-Intervall auf täglich

Options

Enable scheduled scans

☐ No (default)
☐ Hourly
☐ Twicedaily
☒ Daily

Scheduled scan report

☒ Send me a report by email only if changes are detected (default)
☐ Always send me a report by email after a scheduled scan

Save Scan Options

Schritt 17: klick den Speichern-Button

Monitoring Help ▾

Your changes have been saved. ✕

Schritt 18: gehe zu File Guard auf der gleichen Seite

Monitoring Help ▾

Your changes have been saved. ✕

File Check **File Guard**

Enable File Guard Disabled

Save File Guard options

Schritt 19: aktivier File Guard und klick den Speichern-Button

Monitoring Help ▾

Your changes have been saved. ✕

File Check **File Guard**

Enable File Guard Enabled

Real-time detection

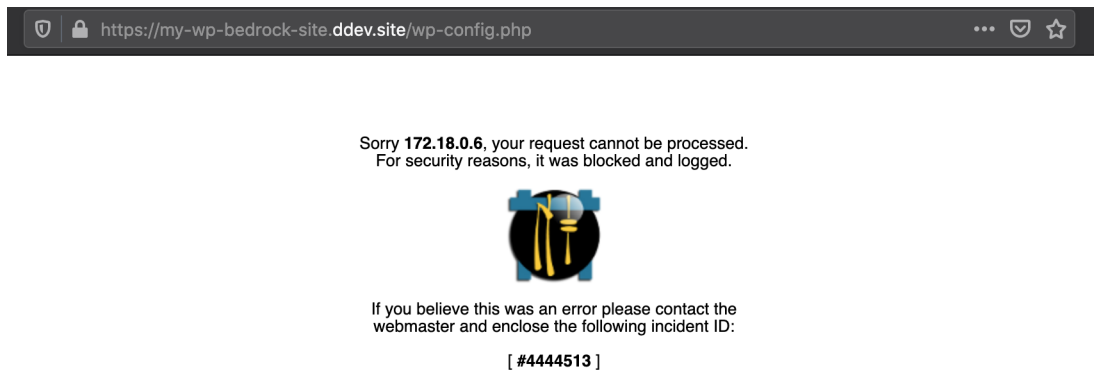
Monitor file activity and send an alert when someone is accessing a PHP script that was modified or created less than hour(s) ago.

Exclude the following files/folders (optional)

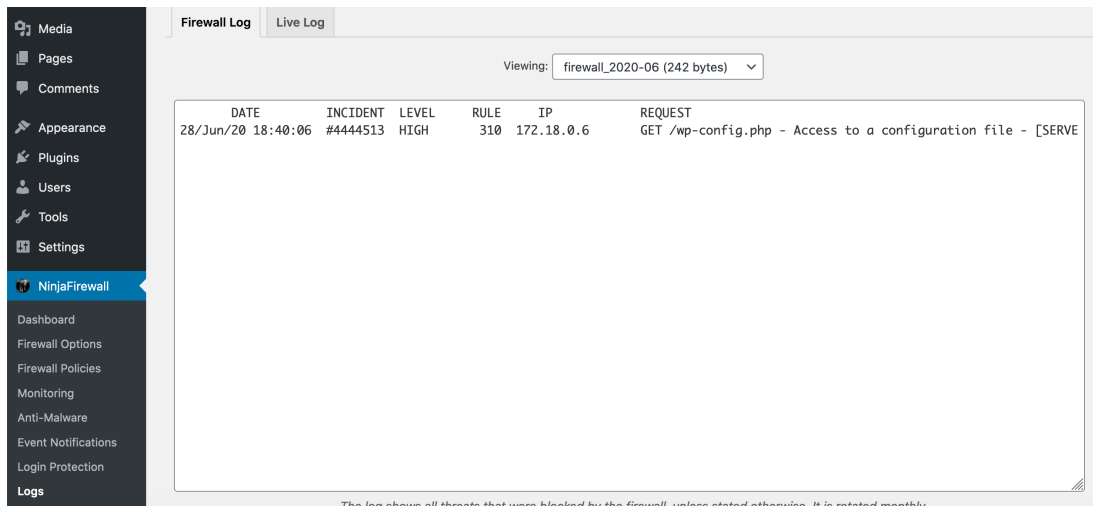
Full or partial case-sensitive string(s), max. 255 characters. Multiple values must be comma-separated (,).

Save File Guard options


Schritt 20: öffne ein neues Inkognito-Fenster im Browser und öffne deine-domain/wp-config.php oder deine-domain/?%00, die Anfrage sollte blockiert sein und dort sollte die folgende Information von NinjaFirewall sein die unten auch die Event-ID enthält



Schritt 21: gehe zu NinjaFirewall – Logs, die blockierte Anfrage sollte jetzt dort auftauchen



Schritt 22 (optional): gehe zu NinjaFirewall – Login Protection und verwende die folgenden Optionen

 **Login Protection**

Enable brute force attack protection

Enabled

Type of protection

☐ Username + Password
☒ Captcha image

When to enable the protection

☒ Always enabled
☐ When under attack

Message

Type the characters you see in the picture below:

This message will be displayed above the captcha. Max. 255 characters.

Various options

Apply the protection to the `xmlrpc.php` script as well

Yes

Enable bot protection

Yes