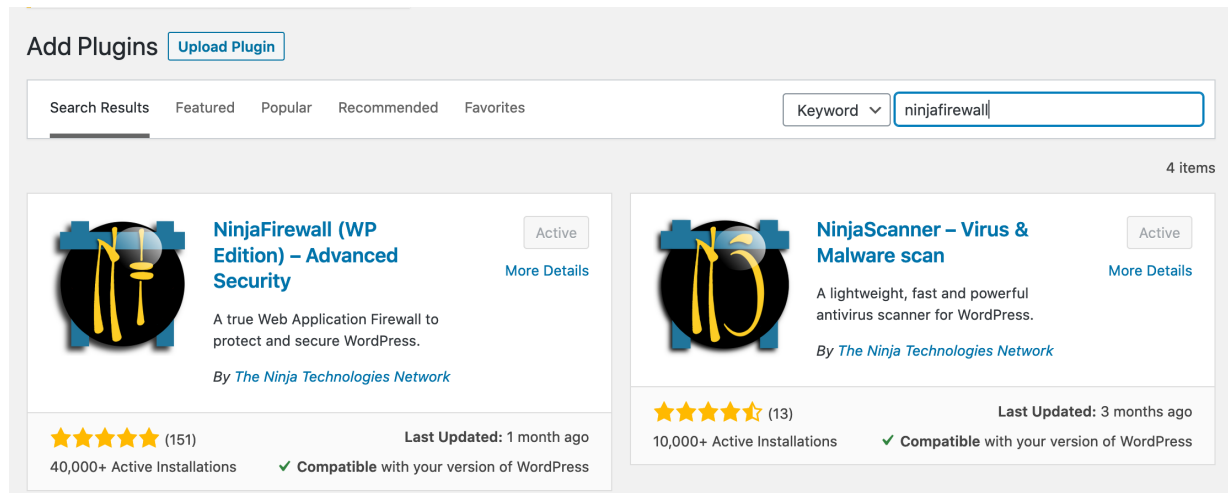
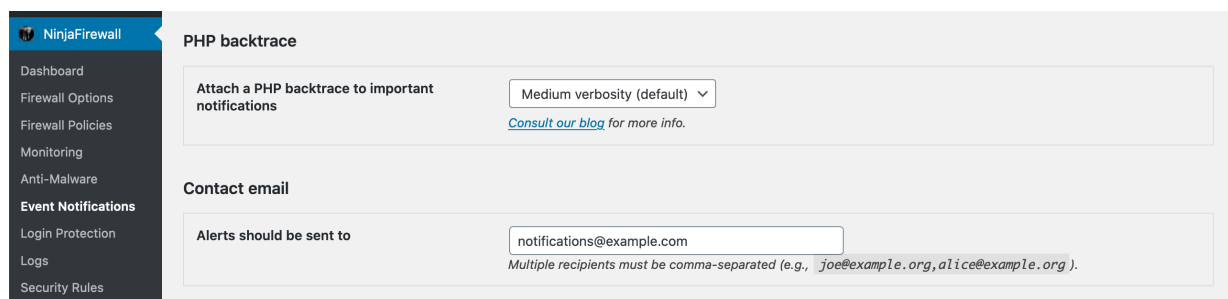


Schritt 1: installiere und aktiviere NinjaFirewall



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

configuration file for NinjaFirewall

Please keep in mind to enable the **Full Wall**
Monitoring (File Check and File

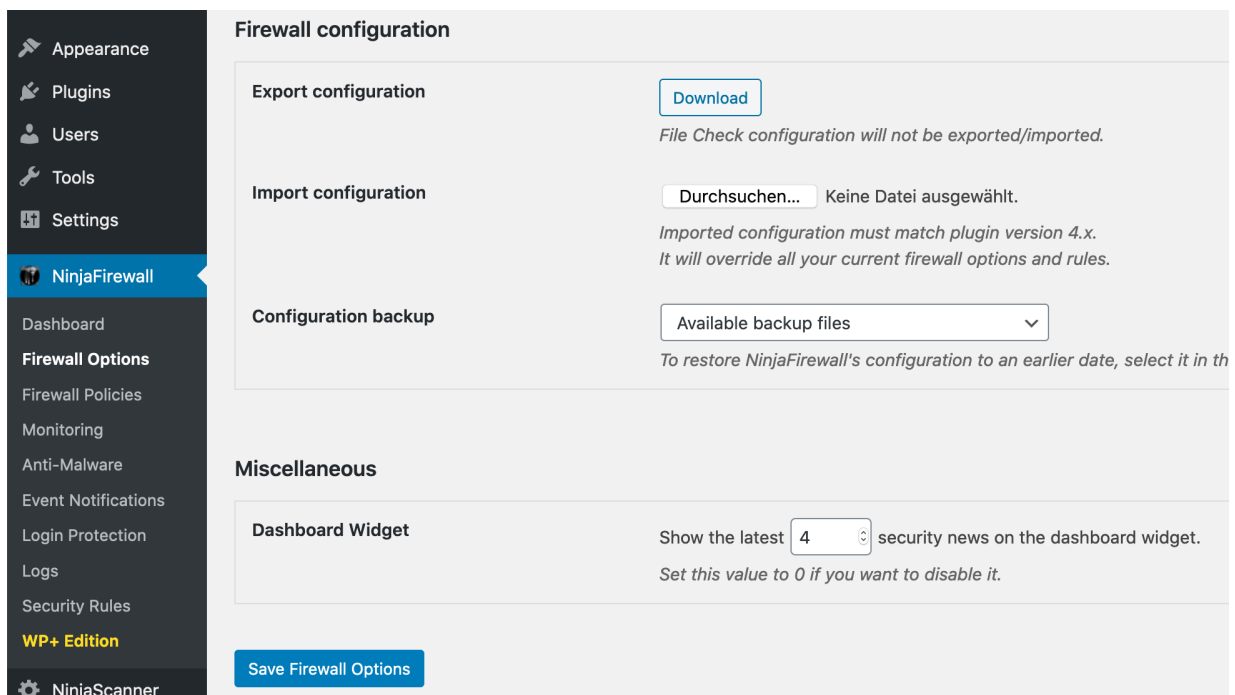
email for notifications in NinjaFirewall

notifications@example.com

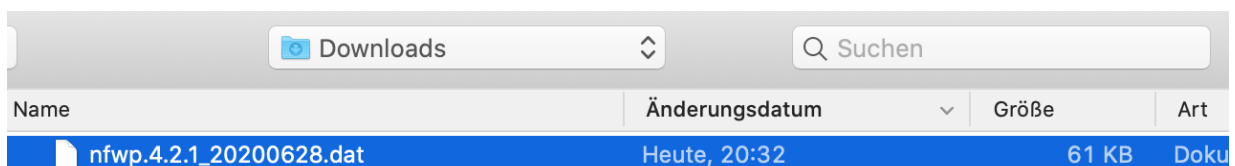
download



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...](#) nfwf.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 Options'.

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)

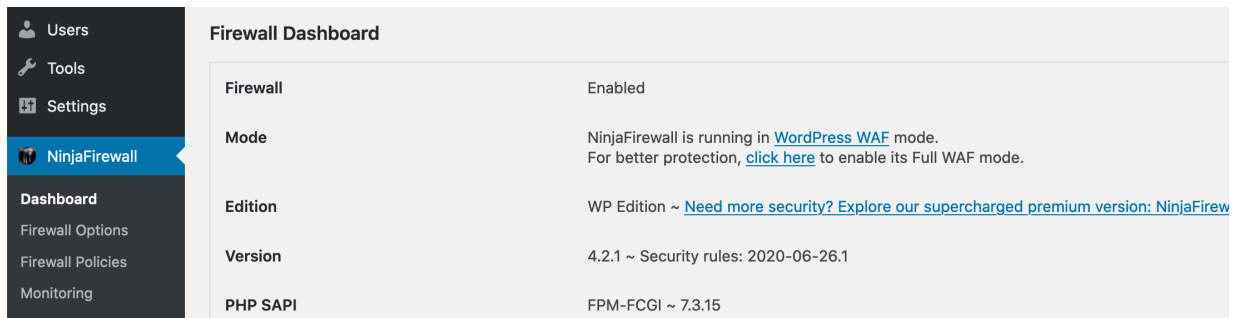
Plugins

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

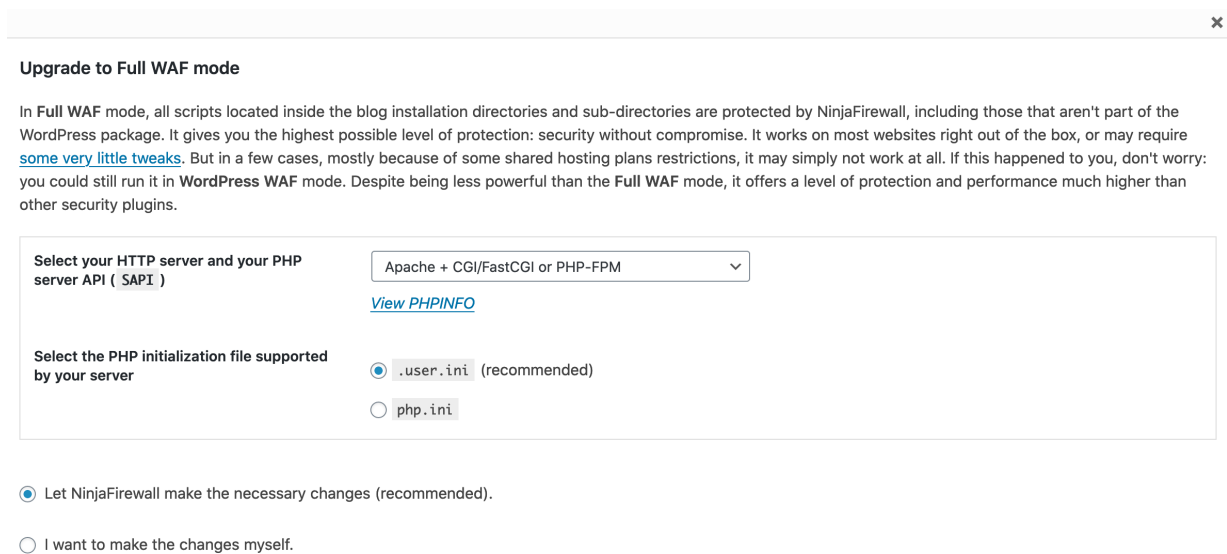
Send me an alert whenever someone ☒ Updates a theme (default)

Schritt 9: gehe zu NinjaFirewall – Dashboard



Firewall Dashboard	
Firewall	Enabled
Mode	NinjaFirewall is running in WordPress WAF mode. For better protection, click here to enable its Full WAF mode.
Edition	WP Edition ~ Need more security? Explore our supercharged premium version: NinjaFirewall
Version	4.2.1 ~ Security rules: 2020-06-26.1
PHP SAPI	FPM-FCGI ~ 7.3.15

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



Upgrade to Full WAF mode

In Full WAF mode, all scripts located inside the blog installation directories and sub-directories are protected by NinjaFirewall, including those that aren't part of the WordPress package. It gives you the highest possible level of protection: security without compromise. It works on most websites right out of the box, or may require [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.

Select your HTTP server and your PHP server API (SAPI)

Apache + CGI/FastCGI or PHP-FPM

[View PHPINFO](#)

Select the PHP initialization file supported by your server

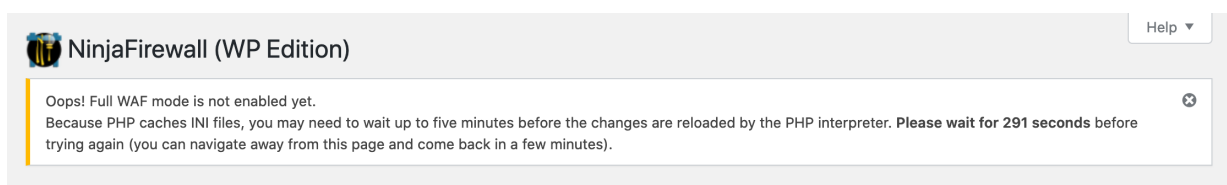
☒ .user.ini (recommended)

☐ php.ini

☒ Let NinjaFirewall make the necessary changes (recommended).

☐ I want to make the changes myself.

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



NinjaFirewall (WP Edition)

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).

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' section with 'File Check' and 'File Guard' tabs. The 'File Check' tab is active, showing instructions: '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.' Below this, there are two input fields:

- Create a snapshot of all files stored in that directory:** The input field contains '/var/www/html/web/wp/'. Below it, the default is noted as 'Default: /var/www/html/web/wp'.
- Exclude the following files/folders (optional):** The input field contains '/app/nfwlog/'. Below it, a note states: 'Full or partial case-sensitive string(s). Multiple values must be comma-separated (,).' There is a checkbox labeled 'Do not follow symbolic links (default)' which is checked.

A 'Create Snapshot' button is located at the bottom of the form.

Schritt 15: erstell einen Snapshot

The screenshot shows the 'Monitoring' section with a success message at the top: 'Snapshot successfully created.' Below this, the 'File Check' and 'File Guard' tabs are visible. The 'File Check' tab shows the 'Last snapshot' 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 these details are two buttons: 'Download Snapshot' and 'Delete Snapshot'. At the bottom, it shows 'Last changes' as 'None' and a 'Scan System For File Changes »' button.

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



Sorry **172.18.0.6**, 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:

[**#4444513**]


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

The screenshot shows the NinjaFirewall dashboard with the 'Firewall Log' tab selected. The log displays a single entry for a blocked request. The left sidebar contains navigation links for various system components.

DATE	INCIDENT	LEVEL	RULE	IP	REQUEST
28/Jun/20 18:40:06	#4444513	HIGH	310	172.18.0.6	GET /wp-config.php - Access to a configuration file - [SERVE

The log shows all threats that were blocked by the firewall, unless stated otherwise. It is rotated monthly.

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