# Fail2Ban

## Inhaltsverzeichnis


- 1. Was ist das Problem?
- 2. Was macht Fail2Ban?
- 3. Wie schützt Fail2Ban deinen Server?
- 4. Ersetzt Fail2Ban eine Firewall?
- 5. Ist Fail2Ban kompliziert?
- 6. Kurz zusammengefasst


Fail2Ban ist ein Sicherheitsprogramm für Linux-Server. Es schützt deinen Server vor automatischen Angriffen, zum Beispiel auf den SSH-Zugang.

## 1. Was ist das Problem?

Server, die aus dem Internet erreichbar sind, werden ständig von Bots angegriffen.
Diese Bots versuchen automatisch:

- Benutzernamen zu erraten
- Passwörter auszuprobieren
- sich per SSH anzumelden

Das nennt man **Brute-Force-Angriffe**.

## 2. Was macht Fail2Ban?

Fail2Ban beobachtet die Logdateien deines Systems, zum Beispiel:

- fehlgeschlagene SSH-Anmeldungen
- falsche Passwörter
- ungültige Login-Versuche

Wenn eine IP-Adresse zu oft hintereinander Fehler verursacht, passiert Folgendes:

1. Fail2Ban erkennt die verdächtigen Login-Versuche
2. Die IP-Adresse wird automatisch gesperrt
3. Weitere Verbindungsversuche von dieser IP werden blockiert

Die Sperre kann zeitlich begrenzt oder dauerhaft sein.

## 3. Wie schützt Fail2Ban deinen Server?

- Es stoppt automatische Angriffe sehr früh
- Es reduziert unnötige Login-Versuche
- Es entlastet deinen Server
- Es arbeitet komplett im Hintergrund

Für normale Benutzer ist Fail2Ban unsichtbar.

## 4. Ersetzt Fail2Ban eine Firewall?

Nein.
Fail2Ban **ersetzt keine Firewall**, sondern ergänzt sie.

- Eine Firewall regelt, **welche Ports erreichbar sind**
- Fail2Ban entscheidet, **wer nach Fehlversuchen ausgesperrt wird**

Zusammen sorgen sie für deutlich mehr Sicherheit.

## 5. Ist Fail2Ban kompliziert?

Nein.
Für Einsteiger ist Fail2Ban besonders geeignet, weil:

- es schnell eingerichtet ist
- sinnvolle Standardwerte mitbringt
- es automatisch arbeitet
- man kaum Wartung hat

## 6. Kurz zusammengefasst

Fail2Ban ist ein automatischer Schutzdienst für Linux-Server, der Angreifer erkennt und aussperrt, bevor sie Schaden anrichten können.