

# Nuova soluzione di filtering Anti Crawler, Bot AI e DDoS

Stato  
Inizio

**Publicato**

2026-05-24 14:24 UTC

Siamo lieti di annunciare la disponibilità di **WAF 4 NGINX**, la nuova soluzione proprietaria di Web Application Firewall sviluppata internamente da Managed Server per proteggere i siti web ospitati sulla nostra infrastruttura da scraper aggressivi, bot AI, attacchi DDoS Layer 7 e traffico automatizzato malevolo.

Il servizio è stato progettato per offrire una protezione robusta senza compromettere l'esperienza degli utenti reali: i visitatori legittimi accedono al sito normalmente, mentre i bot ostili vengono identificati, sfidati o bloccati a seconda della loro pericolosità.



## Funzionalità principali









- **Anti Crawler** — rilevamento e blocco di scraper, indicizzatori non autorizzati, copy-cat tool e bot di estrazione dati. Distingue automaticamente tra crawler autorizzati (Googlebot, Bingbot, Applebot, Facebook Crawler) e bot non desiderati.
- **Anti Bot AI** — mitigazione mirata dei crawler delle principali aziende di intelligenza artificiale: *GPTBot* (OpenAI), *ClaudeBot* (Anthropic), *CCBot* (Common Crawl), *PerplexityBot*, *AmazonBot*, *Google-Extended*, *Bytespider* (ByteDance/TikTok), *FacebookBot*, *Applebot-Extended* e altri agenti che acquisiscono contenuti per l'addestramento di modelli linguistici.

- **Anti DDoS Layer 7** — protezione applicativa contro attacchi volumetrici e slowloris attraverso challenge JavaScript trasparenti, sfide Proof-of-Work, verifica Human Checkbox in stile Cloudflare, e modalità Under Attack attivabile con un click in caso di incidente in corso.
- **Browser Fingerprinting avanzato** — riconoscimento di browser headless, automation tool (Puppeteer, Playwright, Selenium) e ambienti virtualizzati tramite analisi di Canvas, WebGL, AudioContext, font installati, hash matematici e oltre 19 segnali comportamentali.
- **Custom Rules Engine** — motore di regole personalizzabili con condizioni su IP, paese (GeoIP), ASN, continente, User-Agent, URI, query string, header HTTP, content type e altro. Supporta operatori avanzati come matches (regex), wildcard, in\_list, contains\_any, ip\_in\_range (CIDR). Le azioni possibili includono: blocco, challenge, log, rate-limit, allow. Le regole sono gestibili sia globalmente (fleet-wide) sia per singolo dominio.
- **IP Reputation e Threat Intelligence** — tracciamento degli IP malevoli con storico ban, ricerca puntuale, reputation score e analisi geografica delle minacce attraverso una threat map interattiva.
- **Dashboard centralizzata** — pannello di controllo unificato con statistiche in tempo reale, KPI di traffico (Humans vs Bots, Pass Rate, Bot Pressure), notifiche per eventi critici (nodi offline, attacchi in corso, certificati SSL in scadenza), audit log delle modifiche, gestione dei ban e cronologia degli eventi di sicurezza.

Regole Personalizzate

november.example.com Domain Global Deployed 2d ago [Distribuisci Regole](#)

Rules Find Unused Rules Debug from Node + Add Rule

ORDER	NAME	WHEN	ACTION	ACTIVITY 24H	CREATED	UPDATED	ENABLED	ACTIONS
1	Lets Encrypt ACME <span>global</span>	URI Path contains <code>/,well-known/acme-challenge/</code>	allow	 24	2026-05-09 00:53	2026-05-20 16:42	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
2	Sblocco API	URI Path contains any of <code>/api/,webservice/</code>	allow	 1927	2026-05-13 10:40	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
3	PayPal Pagamenti Paypal	User-Agent contains <code>PayPal</code>	allow	 0	2026-05-12 20:35	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
4	Clerk.io	User-Agent contains <code>clerk.io</code>	allow	 2539	2026-05-19 16:00	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
5	ShoppingFeed	User-Agent contains <code>ShoppingFeed</code>	allow	 1465	2026-05-12 15:27	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
6	Multisafepay	User-Agent contains <code>notify/26.7.0</code> OR URI Path contains <code>multisafepayofficial</code>	allow	 0	2026-05-12 15:22	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
7	SOLO ITALIA	Country Code is in list <code>IT,SK,GI,VA</code>	allow	 26.747	2026-05-12 15:01	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>
8	Motive	URI Path contains <code>/module/motive/</code>	allow	 295	2026-05-12 20:38	2026-05-20 12:09	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">View</a> <a href="#">Refresh</a> <a href="#">Delete</a>

8 rules

## Perché è importante contro i bot AI

Nel corso degli ultimi 18 mesi, il traffico generato da crawler delle aziende di intelligenza artificiale è cresciuto in modo esponenziale. Su molti siti dei nostri clienti, questi bot rappresentano oggi una quota significativa del traffico complessivo — in alcuni casi **oltre il 50% delle richieste**.

L'impatto operativo di questa attività è tutt'altro che trascurabile:

- Consumo eccessivo di risorse server (CPU, RAM, I/O di database)

- Aumento dei costi di banda e di erogazione
- Rallentamento delle performance percepite dagli utenti reali
- Acquisizione massiva di contenuti originali, articoli, schede prodotto e dati commerciali senza autorizzazione esplicita
- Rischio di vedere i propri contenuti riutilizzati nei sistemi di AI generativa

**WAF 4 NGINX** identifica selettivamente questi bot — sia tramite User-Agent dichiarato, sia attraverso fingerprinting comportamentale per quelli che cercano di mascherarsi — e li blocca o li sfida secondo la policy configurata, preservando il traffico umano legittimo e i bot dei motori di ricerca tradizionali quando sono utili al posizionamento SEO.

## Regole personalizzate e flessibilità

Il sistema di Custom Rules consente a ogni cliente di costruire policy di sicurezza su misura per il proprio sito. Alcuni esempi pratici di utilizzo:

- Bloccare interi paesi o continenti da cui non si riceve traffico legittimo
- Permettere il passaggio incondizionato dei bot di validazione SSL (Let's Encrypt ACME)
- Imporre challenge più aggressivi (Human Checkbox) sui path di amministrazione di CMS come WordPress, PrestaShop, Magento
- Applicare rate-limit specifici sulle API o sui form di login
- Bloccare User-Agent noti per attività malevola o scraping
- Whitelistare ASN di partner commerciali, monitoraggio interno o servizi terzi affidabili

Le regole sono propagate automaticamente a tutti i nodi del fleet quando vengono create o modificate, garantendo coerenza di policy senza intervento manuale.

New Rule ×

Rule Name:  Priority:   
Lower = evaluated first

Description (optional):

Then:  Challenge Mode:

# When incoming requests match... + Add condition

IP Address equals Value ×

Country Code (IPv4 or IPv6). Use CIDR for ranges ( ).

Continent

ASN

HTTP Method

URI Path

Query String

Full URL

User-Agent

Referer

Accept Header

Cookie

Content-Type

Content-Length

Scheme

HTTP Version

Custom Header...

## Disponibilità del servizio

Il servizio **WAF 4 NGINX** è disponibile con due modalità di accesso:

- **Incluso gratuitamente** per tutti i clienti con soluzioni dedicate o gestite: *VPS, Server Dedicati, infrastrutture Cloud e Server Managed*. Il servizio viene installato, configurato e mantenuto dal nostro team senza costi aggiuntivi.
- **Disponibile come servizio extra opzionale** per i clienti con piani di Shared Hosting. L'attivazione viene effettuata su richiesta e include configurazione iniziale, ottimizzazione e supporto.

Per attivare il servizio, ricevere maggiori informazioni o discutere una configurazione personalizzata per le specifiche esigenze del proprio sito, è possibile contattare il nostro reparto tecnico attraverso l'area clienti o aprire un ticket di supporto.

Per riferimenti consigliamo la seguente lettura : <https://tinyurl.com/3bzafmh>