Protect

zcrWAF

Web Application Firewall

zcrWAF is a Thai-built web application firewall that screens traffic for websites and APIs, blocking OWASP Top 10 attacks and bots before the origin server.

BUILT FOR	Thai organizations · Public websites · E-commerce teams · API owners · IT and security teams
THE OPERATING GAP	Public websites and APIs face OWASP Top 10 attacks, bots, automated scripts, flood attempts, brute-force patterns, and abnormal traffic that can be hard to separate from real users.
COVERS	Websites · Web Apps · APIs · Origin Servers · Bots / Scripts · Organizations
DELIVERY OPTIONS	Cloud / SaaS · Virtual appliance · ICT hardware appliance, chosen in solution design

CORE CAPABILITIES

- OWASP Top 10 and common web attack protection
- Rate limiting for bots, brute force, credential stuffing, web scraping, and Layer 7 DDoS
- Bot and automated scanner protection with abnormal traffic control
- CAPTCHA and authentication challenges for suspicious users and high-risk paths
- Custom Allow, Block, or Challenge rules
- Real-time dashboard, Attack Map, security logs, and backend health visibility
- Real-time alerts through E-Mail, Microsoft Teams, LINE, and Webhook channels
- Multi-tenant policy and dashboard isolation with RBAC, least-privilege access and audit trails

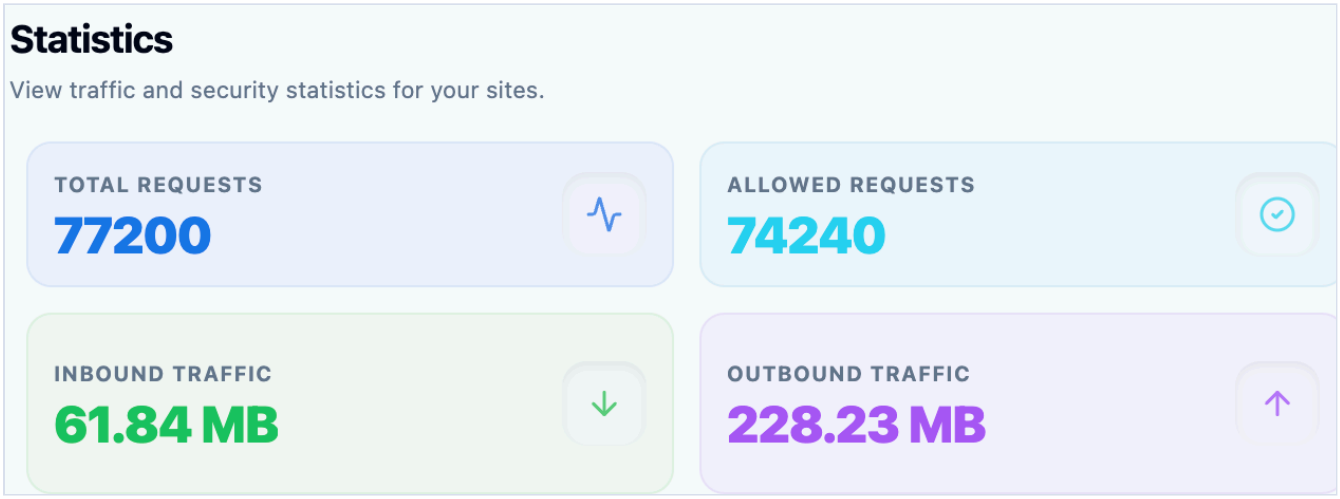
HOW zcrWAF WORKS

Screen and challenge traffic before origin

zcrWAF inspects traffic, applies rate limits and challenges, and monitors attacks in real time.

zcrWAF Outcomes

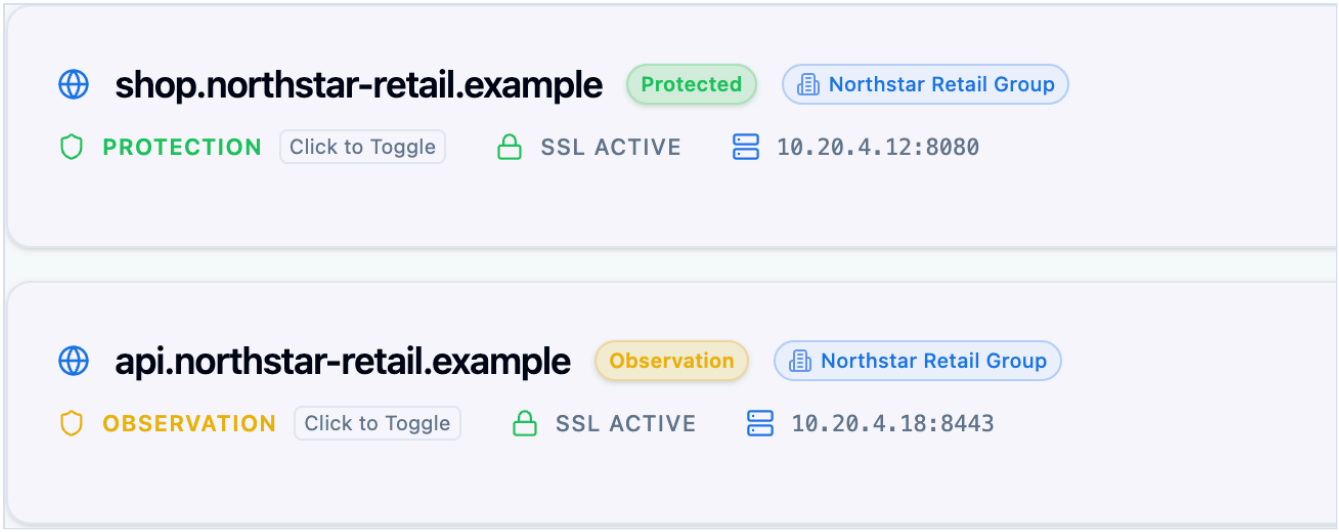
- **Application-Layer Protection** — Block common web attacks and OWASP Top 10 patterns before they reach production systems.
- **Traffic Control** — Limit abnormal traffic, flood attempts, and brute-force behavior without blocking real users blindly.
- **Human Verification** — Use CAPTCHA and authentication challenges on high-risk pages or suspicious sessions.
- **Operational Visibility** — Review security logs, attacks, dashboards, and rule activity in real time.



Selected dashboard widgets: request and traffic totals in a demo environment. These counters are not throughput, attack-prevention guarantees or customer results. Open original capture ↗

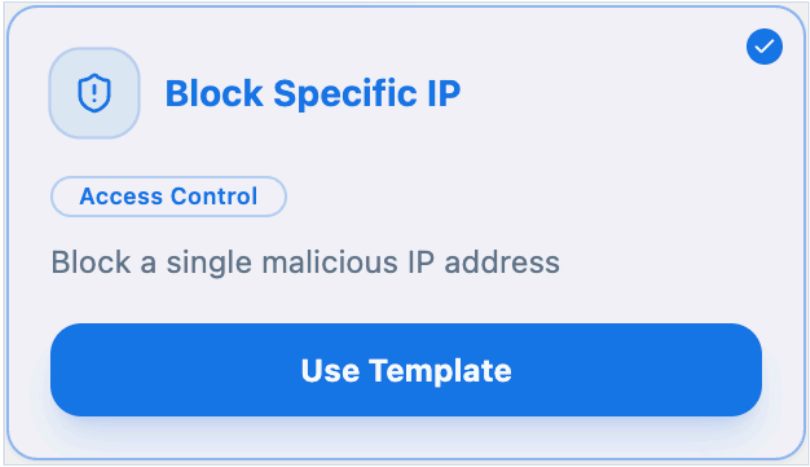
> Illustrative demo data, not customer results, capacity or performance evidence. English UI retained.

01 · Check the site's actual protection state



Two complete site records show Protected versus Observation, SSL state and origin address. Observation is not the same as active protection; the sample names do not identify customers. Open original capture ↗

02 · Review a concrete rule template



The complete Block Specific IP template includes its Access Control category, description and Use Template control. Selecting a template is not proof that a production rule has been deployed. The library also includes templates for admin-page restriction and sensitive-file blocking; see the full original capture. Open original capture ↗

> Illustrative demo data, not customer results, capacity or performance evidence. English UI retained.

zcrWAF FAQ

What deployment options are available?

zcrWAF is available in three deployment options: Cloud / SaaS, Virtual Appliance, and ICT Hardware Appliance for on-premises deployment.

How is zcrWAF priced?

zcrWAF is priced by deployment size, term, and support needs — contact a zcr.ai channel partner for a scoped quote.

What protections are included?

Core protections include OWASP Top 10 coverage, rate limiting, bot and automated traffic protection, CAPTCHA or authentication challenges, real-time monitoring, and logs.

OPERATING AND COMMERCIAL SCOPE

Cloud / SaaS	1-year cloud WAF subscription for up to 3 protected domains.
Virtual Appliance	On-premises virtual appliance with unlimited protected domains and first-year maintenance (MA) included.
ICT Hardware Appliance	On-premises appliance with unlimited protected domains, 1 Gbps GbE throughput, and first-year maintenance (MA) included.

Thai-Developed WAF Operations

zcrWAF is built for organizations in Thailand that need flexible WAF deployment, real-time security logs, maintenance, and security policy tuning.

Support: your channel partner provides first-line support; zcr provides product support to the partner.

Evaluate with an approved partner

Bring protected domains/APIs, origin endpoints, the desired deployment, term and support needs. Your partner validates sizing, maintenance scope and policy-tuning responsibilities in the proposal.

Your approved partner scopes the proposal, quotation, contract and delivery.

Contact a partner ↗ Current packages ↗ Product resources ↗