WAF (Web Application Firewall)

Inhaltsverzeichnis

Eine Web Application Firewall (WAF) filtert HTTP(S)-Traffic zu Webanwendungen und blockiert typische Angriffe wie SQL-Injection oder XSS. Sie ergänzt Netzwerk-Firewalls auf Anwendungsebene.

1 Funktionsweise

Die WAF analysiert Anfragen und Antworten anhand von Signaturen, Regeln und teils Verhalten. Verdächtige Requests werden markiert, challenge'd oder blockiert, bevor sie die Anwendung erreichen.

- **OWASP-Fokus:** Schutz vor gängigen Web-Schwachstellen
- **Virtual Patching:** temporäre Absicherung vor App-Fixes
- **Rate-Limits / Bots:** Missbrauch und Automationen eindämmen

2 Typische Einsatzbereiche

- Öffentliche Websites, APIs und Kundenportale
- Schutz älterer Anwendungen mit bekanntem Risiko
- Zusatzschicht vor Reverse Proxy oder Ingress

3 Wichtige Hinweise

- Falsch positive Regeln können Legitimate Traffic stören – Tuning nötig.
- Eine WAF ersetzt keine sichere Anwendungsentwicklung.
- TLS, Logs und Bypass-Wege müssen mitgedacht werden.

4 Fazit

WAFs erhöhen den Schutz von Webanwendungen spürbar, wirken aber am besten als Teil einer Defense-in-Depth-Strategie – nicht als alleinige Sicherheitslösung.