# WAF (Web Application Firewall)

**WAF** funguje jako inteligentní brána mezi webovou aplikací a internetem. Jeho hlavním účelem je chránit webové servery před útoky, které se snaží zneužít chyby v kódu aplikace, jako jsou SQL Injection, Cross-Site Scripting (XSS) nebo Command Injection.

---

# Jak WAF funguje?

WAF analyzuje každý příchozí požadavek (GET, POST atd.) a porovnává ho se sadou bezpečnostních pravidel:

- **Pozitivní model (Whitelisting):** Povoluje pouze provoz, který odpovídá známým a bezpečným vzorům. Vše ostatní blokuje.
- **Negativní model (Blacklisting):** Blokuje pouze provoz, který obsahuje známé útočné signatury (např. podezřelé SQL příkazy v URL).
- **Analýza chování:** Moderní WAF využívají umělou inteligenci k detekci anomálií, které neodpovídají běžnému chování uživatelů.

---

# Rozdíl mezi WAF a běžným firewallem

| Vlastnost | Síťový Firewall (L3/L4) | Web Application Firewall (L7) |
|---|---|---|
| **Zaměření** | Ochrana sítě a portů. | Ochrana konkrétní webové aplikace. |
| **Co vidí** | IP adresy, protokoly (TCP/UDP), porty. | Obsah HTTP požadavku, parametry formulářů, cookies. |
| **Typy útoků** | DDoS, neoprávněný přístup k portům. | SQLi, XSS, Session Hijacking, zneužití API. |

---

# Formy nasazení

WAF může být realizován několika způsoby:

```
1. **Cloudový WAF:** Služba běžící u poskytovatele (např. Cloudflare,
Akamai). Snadné nastavení, nevyžaduje instalaci na server.
2. **Softwarový WAF:** Modul nainstalovaný přímo na webovém serveru (např.
**ModSecurity** pro Apache nebo Nginx).
3. **Hardwarový WAF:** Samostatné fyzické zařízení umístěné v datovém centru
před servery. Nabízí nejvyšší výkon, ale je nejdražší.
```

---

# Hlavní přínosy

- **Okamžitá ochrana (Virtual Patching):** Pokud je v aplikaci nalezena chyba, WAF ji dokáže zablokovat dříve, než vývojáři opraví samotný kód.
- **Ochrana proti botům:** Dokáže identifikovat a zastavit škodlivé roboty, kteří se pokoušejí o „scrapping“ dat nebo hádání hesel.
- **Compliance (Shoda s předpisy):** Pro mnoho standardů (např. PCI DSS pro platby kartou) je mít nasazený WAF povinností.

---

*Související pojmy: SQL Injection, Command Injection, HTTP, Firewall, Kybernetická bezpečnost, ModSecurity.*