WAF a síťová bezpečnost

V tradičním pojetí bezpečnosti stačilo hlídat hranice sítě. Dnes se však většina útoků odehrává na aplikační vrstvě (L7), kde útočníci zneužívají chyby v kódu webů. **WAF** funguje jako specializovaný filtr, který těmto útokům předchází.

1. Co je to WAF?

Web Application Firewall (WAF) je zařízení nebo služba, která filtruje, monitoruje a blokuje HTTP/HTTPS provoz směrem k webové aplikaci a z ní. Na rozdíl od běžného firewallu, který vidí pouze „obálku“ dat, WAF čte jejich obsah.

Rozdíl mezi Network Firewallem a WAF

Vlastnost	Network Firewall (L3/L4)	WAF (L7)
Vrstva OSI	Síťová a transportní	Aplikační
Co sleduje	IP adresy, porty, protokoly	Parametry URL, Cookies, formulářová data
Ochrana proti	DDoS útoky na linku, skenování portů	SQL Injection, XSS, CSRF
Příklad	Povolí provoz na portu 443	Zkontroluje, zda v poli pro jméno není skript

---

2. Klíčové funkce WAF

WAF využívá různé strategie k identifikaci škodlivého provozu:

- **Detekce na základě signatur:** Porovnávání požadavků s databází známých útoků (např. vzorce pro **OWASP Top 10**).
- **Behaviorální analýza:** Sleduje anomálie v chování. Pokud uživatel odešle 500 formulářů za sekundu, WAF jej vyhodnotí jako bota.
- **Virtual Patching:** Okamžitá blokace provozu zneužívajícího nově objevenou chybu, než vývojáři opraví kód.
- **Custom Rules:** Správci mohou definovat vlastní pravidla (např. povolit přístup do administrace pouze z konkrétních IP adres).

---

3. Další prvky síťové bezpečnosti

WAF nefunguje izolovaně, ale je součástí širšího ekosystému:

IDS/IPS (Intrusion Detection/Prevention)

- **IDS:** Pasivní systém, který detekuje podezřelou aktivitu v síti a varuje správce.

- **IPS:** Aktivní systém, který podezřelý provoz rovnou zahazuje.

VPN (Virtual Private Network)

Vytváří bezpečný „tunel“ skrze nedůvěryhodný internet. Pro webové servery se VPN často používá pro přístup k administrátorským rozhraním a databázím, které nejsou veřejně dostupné.

TLS/SSL Inspekce

Protože většina webového provozu je šifrovaná (HTTPS), útočníci schovávají své skripty do šifrovaných paketů. Moderní firewally a WAF musí provádět **SSL Termination** (dešifrování), aby mohly obsah zkontrolovat.

---

4. Typy nasazení WAF

- **Cloud-based:** (Např. Cloudflare, AWS WAF) Snadná správa, ochrana na okraji sítě (edge).
- **Hardware/On-premise:** (Např. F5 Big-IP) Maximální výkon a kontrola v datovém centru.
- **Host-based:** (Např. ModSecurity) Modul nainstalovaný přímo na webovém serveru (Apache/Nginx).

Související články:

- Virtual Patching pomocí WAF
- Kybernetické hrozby a prevence
- Model OSI a síťové protokoly

Tagy: network security waf firewall ids ips vpn tls ssl