WAF a síťová bezpečnost

V moderní síťové architektuře již nestačí pouze hlídat porty a IP adresy. Útoky se přesunuly do aplikační vrstvy. **WAF** (Web Application Firewall) je klíčový prvek, který analyzuje komunikaci mezi webovou aplikací a internetem a chrání ji před zneužitím.

1. Co je to WAF?

WAF je specifický typ firewallu, který filtruje, monitoruje a blokuje HTTP/HTTPS provoz směrem k webové aplikaci. Zatímco běžný firewall funguje jako brána (hlídá, kdo vchází), WAF funguje jako inspektor obsahu (hlídá, co návštěvník uvnitř dělá).

Rozdíl mezi Network Firewallem a WAF:

- **Network Firewall (L3/L4):** Rozhoduje na základě IP adres a portů (např. povolí port 80/443). Neřeší, co je obsahem dat.
- **WAF (L7 - Aplikační vrstva):** Rozumí struktuře webových požadavků. Dokáže rozpoznat SQL Injection ukrytou v URL nebo škodlivý skript ve formuláři.

—

2. Jak WAF chrání aplikace?

WAF využívá různé sady pravidel a modelů chování k identifikaci hrozeb:

- **Pozitivní bezpečnostní model (Allowlist):** Povoluje pouze známý, bezpečný provoz a vše ostatní blokuje.
- **Negativní bezpečnostní model (Blocklist):** Využívá signatury známých útoků (např. vzorce pro **OWASP Top 10**) a blokuje je.
- **Behaviorální analýza:** Sleduje anomálie v chování uživatelů (např. příliš rychlé procházení stránek, které indikuje bota).

—

3. Klíčové funkce síťové bezpečnosti

Kromě WAF zahrnuje komplexní síťová bezpečnost další technologie:

IDS/IPS (Intrusion Detection and Prevention Systems)

- **IDS:** Detekuje podezřelou aktivitu a informuje administrátora.
- **IPS:** Aktivně zasahuje a blokuje útoky v reálném čase na síťové úrovni (např. detekce exploitů v

protokolech SMB, DNS).

VPN (Virtual Private Network)

Vytváří šifrovaný tunel pro bezpečný přenos dat skrze nedůvěryhodné sítě (internet). Zajišťuje integritu a důvěrnost dat.

TLS/SSL Inspekce

Protože většina útoků je dnes šifrovaná (HTTPS), musí být bezpečnostní prvky schopny (za určitých podmínek) dešifrovat provoz, zkontrolovat jej na přítomnost malwaru a znovu zašifrovat.

—

4. Typy nasazení WAF

- **Cloud-based WAF:** (Např. Cloudflare, AWS WAF). Snadné nasazení pomocí změny DNS, nevyžaduje instalaci HW.
- **Hardware WAF:** Fyzické zařízení v datovém centru. Nabízí nejvyšší výkon a kontrolu.
- **Software / Host-based WAF:** Modul přímo na webovém serveru (např. **ModSecurity** pro Apache/Nginx).

—

5. Ochrana proti DDoS

WAF hraje zásadní roli v ochraně proti **DDoS útokům** na aplikační vrstvě (tzv. HTTP floods). Díky schopnosti validovat HTTP hlavičky a cookies dokáže odlišit reálného uživatele od botnetu, který se snaží přetížit server.

Související články:

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

Tagy: network security waf firewall ids ips ddos vpn tls