Web 应用防火墙（WAF）技术演进与发展趋势

文◆贵州师范大学 大数据与计算机科学学院 龙安康 罗 云

引言

当前，Web 应用已成为企业、政府乃至个人日常活动的重要载体，其安全性将会直接影响一个国家数字经济的稳定与繁荣。WAF 作为一种专门针对 Web 攻击的关键防御手段，自其诞生以来，始终处于网络安全防护技术发展的前沿。然而，面对日益复杂的网络威胁环境、快速演进的技术架构以及相关法律法规的完善，WAF 技术面临着前所未有的挑战与变革需求。本文系统性地探讨 WAF 技术的演进历程及其未来发展趋势，有助于增加对保障 Web 应用的安全性、提升整体网络防御水平的理解，并为政企在数字化旅程保驾护航。

1 历史回顾

WAF 的发展历程反映了网络安全领域对 OSI 应用层防护的需求增加与技术创新。传统的网络防火墙主要在 OSI 网络层与传输层进行安全防护，对于 HTTP 等应用层协议的内容包无法进行识别。因此 WAF 填补了传统防火墙在应用层防护方面的空白。

1.1 初始探索与市场兴起

2004 年，国外一些安全厂商提出了 Web 应用防火墙，但当时很多企业用户对此认识比较模糊 [1]。这一提议的背后，是企业对传统防火墙在应用层防御局限性的认识。鉴于此，企业界逐渐意识到亟需更有效的解决方案应对应用层的威胁。美国梭子鱼网络公司正是在这种背景下，为了弥补市场空白，提出了针对 HTTP 流量进行细致分析的方案。该方案通过深入检测 HTTP 请求内容，精细分析并对危险请求进行拦截，有效抵御 SQL 注入、跨站脚本（XSS）等应用层攻击。这一阶段，WAF 市场初步形成，产品形态多为硬件设备或软件插件，主要服务于大型企业与特定行业用户。

1.2 功能扩展与标准化进程

随着 Web 应用复杂性的不断增加以及 WAF 向大众的普及，WAF 不再是企业及相关行业的专属。传统的系统内置 WAF 已无法满足用户需求，WAF 开始集成更多安全功能，如 CC 攻击防护、内容审查、访问控制等。2006 年，Web 应用安全联盟发布《Web 应用防火墙评价标准》，对于 Web 应用防火墙的研发起到了指导作用 [2]。这一阶段 WAF 逐步从单一防护工具转变为综合安全平台，形成了协同防御体系，增强了对复杂威胁场景的适应能力。

1.3 云化转型与 AI 赋能

云计算自 2006 年被谷歌公司正式提出后，推动了 WAF 向云服务模式地转变。云计算具有的按需自动取用、资源利用率高、业务承载能力强、弹性敏捷、扩展性好等优势迅速获得市场青睐 [3]。此外，随着 DevOps 与微服务架构的广泛应用，WAF 开始与 CI/CD 流程深度融合，实现自动化部署与持续防护。学者徐军 [4] 强调，云 WAF 不仅简化了部

【作者简介】龙安康（2001—），男，贵州三穗人，本科，研究方向：Web 安全。
【通讯作者】罗云（1985—），男，四川资中人，硕士研究生，讲师，研究方向：物联网应用。

署流程，还添置了一系列超越传统 WAF 范畴的防护与性能加速特性，囊括了强大的 DDOS 攻击抵御机制以及集成 CDN（内容分发网络），以实现全球范围内的内容加速分发，全方位提升了网络安全的防护度与用户体验的流畅度。

近年来，人工智能技术发展迅猛，在 WAF 领域的应用日益广泛，如利用数据挖掘与分析技术识别攻击威胁特征，主动发现网络中是否存在攻击威胁 [5]。学者朱思猛、杜瑞颖等人 [6] 设计了基于 RNN 的 Web 应用防火墙自动加固方案，使 AI 赋能的 WAF 拦截率达到 90% 以上且误报率为 0，标志着防护技术从规则驱动向数据驱动的重大转变，显著降低了误报率，提高了威胁响应效率。

2 技术原理与功能演进

WAF 的技术原理与功能演进反映了在应对日益复杂 Web 威胁环境中的持续创新与适应性提升。从最初基于规则的静态防护，到如今融合人工智能的动态防御体系，WAF 在技术原理与功能上实现了跨越式的演进进程。

2.1 基于规则的静态防护

正则表达式匹配属于模式匹配，能在给定的字符串中匹配出符合特定规则的字串，由于正则表达式能灵活地对字符串进行处理，所以基于规则策略的静态防护对已经发现的攻击手段有较好的保护作用 [7]。规则策略可以分为白名单和黑名单，前者表示跳过检测，后者表示阻止请求或响应 [8]。黑名单用来防御已知的恶意行为，黑名单中的规则是被认为可疑的 URL 地址、HTTP 头信息、请求参数或其他危险特征，当 WAF 检测到黑名单中的任何元素发起请求时，都会阻止这些请求到达服务器执行。与黑名单相反，白名单只允许规则中的元素通过。这两种模式相结合提供了更为精细的访问控制，且较易实现，但也存在误报率较高的问题，难以应对未知威胁。规则的更新需要依赖于安全团队手动操作或定期补丁，响应速度有限，存在滞后性。

2.2 动态分析与行为建模

为应对规则依赖的局限性，WAF 开始引入动态分析与行为建模技术。张恬 [9] 提出了一种特异性配置的 WAF，根据需要防护的 Web 应用合理有效地配置所需的防护。以 Web 应用本身业务作为切入点，通过合法通信，采集数据样本，变成适应自身业务系统的规则库，更有针对性。通过监测请求特征、会话行为、用户代理信息等，WAF 能够识别异常流量模式，提升对未知威胁的检测能力。动态分析使 WAF 能够根据攻击者行为动态调整防护策略，提高了防护的灵活性与准确性。

2.3 人工智能（AI）驱动与云防护

得益于硬件计算能力的不断增强，AI 技术尤其是深度学习、机器学习在 WAF 中的应用成为重要趋势 [10]。传统的防御手段因其仅能甄别特定的网络入侵行为，无法智能化、动态化地应对复杂的网络入侵行为，已经难以满足当下需求 [11]。学者丁顺莺 [5] 采用一种先进的模式识别算法，该算法基于深度置信网络（Deep Belief Network，DBN）模型，有效提升了识别能力。AI 技术赋能了 WAF 的威胁识别能力，降低了误报率，实现了自适应防护策略的生成与优化。

2008 年，趋势科技首次提出了云安全概念。将域名的 DNS 解析权交给安全商或通过 CNAME 方式解析到安全商，即可无需安装 WAF 软件，使用 CDN（Content Delivery Network）的方式。Web 访问流量经过安全商的清洗后再回源至源主机，避免直接暴露源服务器 IP 至公网。云 WAF 利用黑客攻击样本库和漏洞记录，动态更新防御策略。云厂商同时架设数千台防护设备和骨干网络、安全替身、攻击可追溯性等前沿技术，根据流量需求自动扩展，有效地帮助用户抵御了 DDOS 攻击。然而，这种方式导致用户信息暂存或保存在云服务提供商的服务器中，引发用户对数据隐私泄露的担忧。尽管大多数厂商都有严格的隐私政策和安全措施，用户仍需深入了解数据的具体存储位置及其保护机制，以确保信息的最高安全标准。

3 性能效率改进

WAF 的效率直接影响到网络服务的质量和安全，所以性能与效率改进是其技术演进的重要组成部分，旨在确保高效、低延迟的网络流量处理，同时不影响 Web 应用程序的正常运行。从算法优化到云原生架构地采用，WAF 在提升性能与效率方面取得了显著进展。

3.1 软件优化与并行计算

随着软件定义安全（SDS）理念的兴起，WAF 开始转向软件优化以提高性能。多线程处理、负载均衡、缓存技术的应用以及对复杂规则集的并行计算，显著提升了 WAF 的处理效率。因此，

软件优化不仅降低了硬件成本，还赋予了 WAF 更高的可扩展性和灵活性。

3.2 云原生架构与容器化部署

云技术的普及推动了 WAF 向云原生架构的演进。容器化部署、微服务架构的应用，使 WAF 能够快速弹性伸缩，按需分配资源，以应对瞬时高流量冲击。云 WAF 方案在防护引流拓扑上设计了 SDN 牵引流量和策略下发分离，实现了 WAF 的并发防护调用，解决了传统方案防护吞吐量低的问题 [12]。云原生 WAF 不仅让性能得到了提升，还简化了运维管理，实现了与云环境的深度融合。

3.3 缓存策略与智能调度

新一代 WAF 采用了精细化缓存策略与智能调度机制，如基于风险评分的请求优先级划分、热点内容缓存等，进一步降低了处理负担，提高了整体吞吐量，优化了 WAF 资源利用率，确保了在大规模攻击场景下的稳定服务。AI 技术在 WAF 中的应用不仅提升了威胁检测能力，还有助于性能优化。AI 通过学习流量模式，预测高峰时段，提前动态调整资源分配，减少响应时间。此外，AI 辅助的性能优化有助于实现 WAF 的自适应服务质量和高效能运行。

结语

本文深入探讨了 WAF 软件的发展历程，从基于规则匹配的静态防御到如今基于 AI 的动态防御以及从独立到云原生服务、单一功能到综合平台的演进。WAF 通过云化部署、容器化服务，成功融入现代云环境，提供弹性伸缩、细粒度防护和自动化运维能力，以满足微服务架构的安全需求。

未来，AI 技术将在 WAF 中起到主导作用，不断提升威胁检测与响应的智能化程度，助力精准策略生成、自动漏洞管理等高级功能，实现防护效能的整体提升。WAF 将更加注重隐私保护与合规性，集成更多隐私增强技术，提供更精细的隐私控制选项，助力企业构建合规、可信的 Web 应用服务体系。因此，企业与研发机构应加大投入，研发适应云原生环境、深度融合 AI 技术、高度集成隐私保护功能的新一代 WAF 产品，以提升产品的核心竞争力与市场适应性。安全商则应积极采用先进的 WAF 解决方案，结合自身业务特点与安全需求，实施定制化的防护策略，并加强安全人员培训，以提升应对新兴威胁与复杂攻击的能力。政策制定者应密切关注 WAF 技术发展对法规遵从与隐私保护的影响，适时修订相关法律法规与标准，引导和支持企业采用合规、高效的 WAF 产品与服务，共同营造安全、健康的网络空间。

引用

[1] Web应用防火墙来势汹汹[J].电力信息化,2009,7(7):19.

[2] 王言伟.基于Nginx的Web应用防火墙的设计与实现[D].北京:北京邮电大学,2018.

[3] 陈颖,王普.云计算网络安全管理路径优化[J].湖南邮电职业技术学院学报,2024,23(1):69-72.

[4] 何军.基于云计算的Web防御系统研究[J].网络安全技术与应用,2017(3):81-82.

[5] 丁顺莺.基于深度学习的大数据网络安全防御模式研究[J].信息与电脑(理论版),2018(17):194-195.

[6] 朱思猛,杜瑞颖,陈晶,等.基于循环神经网络的Web应用防火墙加固方案[J].计算机工程,2022,48(11):120-126.

[7] 王言伟.基于Nginx的Web应用防火墙的设计与实现[D].北京:北京邮电大学,2018.

[8] 熊琅钰.基于Nginx的高性能WAF的设计与实现[D].南京:东南大学,2022.

[9] 张恬.Web应用防火墙在高校网络安全中的应用[J].无线互联科技,2022,19(9):116-118.

[10] 徐恩庆,张琳琳,吴佳兴.人工智能赋能政府采购转型升级[J].中国招标,2023(12):15-17+29.

[11] 周路明,郑明才.基于深度学习的网络入侵防御技术研究[J].微型电脑应用,2020,36(11):93-97.

[12] 何丹,张悦.高性能公有云WAF安全方案[J].计算机系统应用,2020,29(4):144-149.