基于多因子权重与日志分析的 WAF 安全策略动态适配机制研究

许俊龙[1] 徐爱华[1] 王 松[1]
XU Junlong XU Aihua WANG Song

摘 要 随着 Web 应用在组织数字化进程中的核心地位日益凸显，其面临的应用层安全威胁也愈发复杂。Web 应用防火墙（web application firewall, WAF）作为应用层防护的关键技术，能够有效应对各种非法攻击，但其依赖静态规则的防护模式存在滞后性，难以有效应对未知威胁。文章基于 WAF 的三元组模型（协议拦截、深度解析、策略执行），通过对 WAF 日志的行为模式挖掘，实证评估了 WAF 在防御目录遍历、Hypertext Preprocessor（PHP）反序列化漏洞等攻击中的实际效能。在此基础上，创新性提出一种基于多因子权重计算模型的动态防护策略适配机制，该机制引入业务属性、时空上下文、实时威胁情报等非技术性因子，构建了一套轻量级、自适应的决策引擎，实现了安全策略从静态预置到动态智能调优的演进。

关键词 Web 应用防火墙；多因子权重计算模型；非技术引擎；动态适配

doi：10.3969/j.issn.1672-9528.2026.05.025

0 引言

随着智慧网络的泛在化发展和数字技术的深度应用，万维网（Web）已演进为社会组织数字化重构的关键支撑平台。然而，网络架构的开放性特征与协议设计中存在的内生性安全漏洞，致使组织在数字化转型过程中面临着技术可信性保障与业务连续性风险并存的复合型安全挑战。当“数据跨越个人边界到群组、兴趣社区、州际、国家甚至全球范围时，在保护数据的完整性和维护隐私策略方面已经遇到复杂的挑战”[1]。据国家信息安全漏洞库（China national vulnerability database, CNVD）统计，2021 年我国政府机构及重要信息系统发生网络安全事件 17 982 起，其中应用层攻击占比达 68.3%[2]。CPR 发布的有关 2022 年网络攻击趋势的新数据报告显示，全球网络攻击频次同比增加 38%，教育、政府和医疗行业成为重灾区[3]。在此背景下，构建一套智能化的网络安全防护体系，确保组织基础数据的安全与完整，成为各组织和安全机构亟待解决的课题。

1 WAF 技术框架与部署策略

作为面向 Web 服务架构设计的专业化安全设备，Web 应用防火墙（web application firewall, WAF）依托开放式系统互联模型（open system interconnection reference model, OSI）第七层协议栈深度解析能力，通过双向流量清洗、协议合规性验证及语义级行为分析，实现对超文本传输（安全）协议（hypertext transfer protoco secure, HTTP(S)）通信流量的精细化监控。相较于网络层防火墙和入侵防御系统（intrusion prevention system, IPS），WAF 具备三重核心优势：一是纵深防御的维度延伸至应用逻辑层；二是防护粒度细化为会话级语义规则；三是威胁检测聚焦开放 Web 应用安全项目（open web application security project, OWASP）Top 10 攻击模式，特别是针对 SQL 注入（structured query language injection, SQLi）、跨站脚本（cross-site scripting, XSS）及敏感信息泄露等应用层威胁的精准阻断。在部署架构层面，WAF 支持硬件设备、软件模块、云服务等多形态实现方式，并可根据业务连续性要求选择在线部署模式（Inline）或带外监测模式（out-of-band）。鉴于组织数据资产呈现非线性扩展、数据价值的幂律分布和数据敏感度的谱系分化的多模态异构特征，组织在部署 WAF 时，需要构建一个涵盖安全防护等级、技术兼容性及演进趋势等关键维度的评估矩阵。同时，相应的 Web 应用安全框架也应当遵循自适应匹配的构建原则，即安全控制措施与业务关键性、数据敏感性、威胁暴露面之间相匹配，如表 1 所示。

表 1 典型行业安全风险及 WAF 应对策略矩阵

行业	核心风险	WAF 策略重点	典型攻击类型
金融	交易数据泄露、支付欺诈	严格参数校验、高频交易监控	SQL 注入、撞库攻击
医疗	患者隐私泄露、系统宕机	敏感数据脱敏、DDoS 防护	勒索软件、数据爬虫
政府	数字主权篡改、高级持续性威胁	国密算法支持、白名单机制	0 day 漏洞利用、社工攻击

1. 南京市科技信息研究所 江苏南京 210018

2 WAF 核心工作机制实证分析

WAF 的核心工作机制可归纳为流量监控三元组模型：协议拦截、深度解析和策略执行。该机制通过构建策略执行平面（policy enforcement plane, PEP）来实现动态检测、实时响应和状态感知。

2.1 协议拦截

WAF 的协议拦截主要是通过 HTTP(S) 协议标准来验证请求端报文的合法性，拒绝包含非法方法或畸形数据包的请求，从而阻断协议层面的攻击。以表 2 为例，在反向代理模式下，WAF 通过网络协议栈旁路截获技术建立 TCP 会话通道，捕获网络四元组信息（客户端 179.43.191.193:32818、服务端 10.10.2.64:80）。协议解析引擎对 HTTP/1.1 报文进行深度结构化拆解，在 POST /adxmlrpc.php 请求头中识别出 XML-RPC 接口反序列化漏洞特征，从而触发 OWASP ModSecurity 核心规则集 1050003 并实施毫秒级阻断（HTTP 403），最终在日志中完整保留了涵盖攻击类型（PHP 反序列化漏洞利用）、恶意数据（a:1:{S:4:\x22what\x22;O:11:\x22Pdp\x5cUri\x5cUrl\x22:1:{S:17:\x22\x5c00Pdp\x5c5CUri\x5c5CUrl\x5c00host\x22;O:21:\x22League\x5cFlysystem\x5cFile\x22:2:{S:7:\x22\x5c00*\x5...']）以及其他攻击向量信息（源 IP、请求时间、请求方法等）。另外，通过 IP:179.43.191.193 安全管理人员可以对请求端进行网络溯源；依据 Host 头 www.njsoft.cn 和 URL 路径 /adxmlrpc.php 映射至暴露的 XML-RPC 服务接口，可以了解外部请求所针对的具体服务和资源，为后续判断攻击行为是否针对特定服务提供基础。

表 2 PHP 反序列化漏洞利用攻击示例

字段	值 / 内容
日期时间	2024/8/30 3:13:09
严重程度	“High”,# 安全事件级别为高风险 #
客户端	179.43.191.193：32818 # 源 IP 及端口 #
服务器	10.10.2.64：80 # 目标 IP 及端口 #
Host 头	www.njsoft.cn # 目标域名 #
URL	/adxmlrpc.php # 目标路径 #
状态码	403
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
事件类型	PHP 反序列化漏洞利用
规则 ID	1050003,# 规则 ID#
动作	拒绝
详细内容	MatchedData: found within ARGS_POST: <?xml version:\x221.0\x22 encoding = \x22ISO-8859-1\x22?> <methodCall> <methodName> openads.spc </methodName> <params> <param> <value> <struct> <member> <name> remote_addr </name> <value> 8.8.8.8 </value> </member> <member> <name> cookies </name> <value> <array> </array> </value> </member> </struct> </value> </param> <param> <value> <string> a:1:{S:4:\x22what\x22;O:11:\x22Pdp\x5cUri\x5cUrl\x22:1:{S:17:\x22\x5c00Pdp\x5c5CUri\x5c5CUrl\x5c00host\x22;O:21:\x22League\x5cFlysystem\x5cFile\x22:2: {S:7:\x22\x5c00*\x5...']
请求头检测过程	POST /adxmlrpc.php HTTP/1.1

2.2 深度解析

WAF 基于 RFC 7231 规范对报文进行语义级的逆向解析，通过递归解码 URL 编码（如将 %2e%2e 还原为路径跳转符 ../）、Base64 嵌套等混淆技术，从元数据中提取出请求方法、资源路径及参数体等结构化数据。表 3 中，WAF 对请求行 GET/cgi-bin/.%2e/%2e%2e/.../etc/hosts 中的百分号编码进行还原，这表明攻击者试图通过 %2e（ASCII “.”）与 %2e%2e（ASCII “..”）的复合编码手法，构造出具有 7 级目录回退特征的恶意路径，即 ../../../../../../../../etc/hosts。同时 WAF 验证 HTTP 版本 HTTP/1.1 的合法性以确保协议合规性；头部解析显示 Host 值 202.127.12.66 被确认为有效 IP 地址格式，User-Agent 值 Lkx-Apache2449 TraversalPlugin/0.0.1 则匹配到已知恶意工具特征库，其内嵌的国际域名 https://leakix.net 和社交账号 https://twitter.com/HaboubiAnis 可能会触发对具有区域性特点的组织业务的非授权访问请求的安全策略审查；示例中的请求报文并未携带参数，但 WAF 仍会对报文的隐藏参数、URL 编码错误（如未闭合的编码字符）或特殊字符注入等潜在风险进行深度检测，由于本例攻击载荷集中于路径遍历，参数部分未发现明显异常。最终，WAF 通过多维度多层次的协议解析与规则匹配实现了对非授权区域攻击的精准拦截。

表 3 目录遍历攻击日志示例

字段	值 / 内容
日期时间	2025-03-04 22:38:37
严重程度	高
客户端	179.43.168.146：39172
服务器	202.127.12.66：80
Host 头	202.127.12.66
状态码	403
User-Agent	Lkx-Apache2449TraversalPlugin/0.0.1 (+https://leakix.net/, +https://twitter.com/HaboubiAnis)
事件类型	路径遍历攻击 (DIR) LocalFileInclusion(LFI)
规则 ID	1030023(路径遍历攻击利用服务器或应用程序漏洞，使攻击者可以获取目录结构，读取、写入任意路径上的敏感文件，并最终在服务器上执行命令。本规则匹配 ../ 等字符。)
动作	拒绝
详细内容	MatchedData:foundwithinREQUEST_FILENAME:cgi-bin/../../../../../../../../../etc/hosts
请求头检测过程	GET/cgi-bin/%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/ hostsHTTP/1.1Host:202.127.12.66User-Agent:Lkx-Apache2449TraversalPlugin/0.0.1 (+https://leakix.net/ + https://twitter.com/HaboubiAnis) Accept-Encoding: gzipConnection:close”

2.3 策略执行

策略执行是 WAF 工作的核心阶段，WAF 依据解析的结构信息，对照预先设定的安全策略进行匹配验证。通过解析还原的数据，WAF 发现请求路径 /cgi-bin/../../../../../../../../../etc/hosts 中包含大量“../”序列，这与 WAF“路径遍历（DIR）”规则（如表 4 所示）相匹配，确认这种不断返回上级目录以访问敏感文件的行为属于目录遍历攻击，触发“1030023”规则，因为正常的业务请求“cgi-bin”目录下的合法操作通常不会涉及访问“/etc/hosts”文件且不会通过多层级向上回溯目录访问文件系统，所以 WAF 认定该请求为恶意的目录遍历攻击并采取阻断措施（HTTP 403）。由于表 2 中 User-Agent 字段值还包含了两个国际域名链接“https://leakix.net/”和“https://twitter.com/HaboubiAnis”，安全管理人员还要把组织的业务对象的拓扑分布、应用周期等非技术属性作为重要的考量因素纳入新的安全架构设计中来，根据业务主体独有的时空特征来构建一套适配组织本身的社会性安全策略，使用“非技术引擎”规则对类似于表 4 中的非法请求进行更加严格的审核和限制。

表 4 WAF 安全策略 1030023 规则表

规则 ID	规则名称	严重程度	精准度	特征	动作
1030023	路径遍历	高	高	匹配 ../ 等字符	阻断

3 动态适配机制

WAF 日志不仅是攻击行为的“数字指纹”，更是实现动态适配机制的战略资源。组织可以通过多维度的日志分析，依循系统、主机、服务和攻击 / 漏洞 4 层次安全威胁评估模型，采取由下及上，先局部后整体的策略 [4]，持续完善“检测 - 响应 - 修复”的闭环防护机制。传统 WAF 防护策略通常基于“已知对已知”, 即依赖既定规则应对已知漏洞或签名（Known-to-Known），难以有效应对“已知对未知”（已知策略对未知漏洞）型威胁，更无法实现“未知对未知”（Unknown-to-Unknown）场景下 AI 驱动的智能检测。

动态适配机制克服了基于静态特征码匹配的传统策略的缺陷。该机制将业务属性与实时安全态势纳入决策过程，通过构建一个基于多因子权重计算的动态适配模型，实现网络空间的拟态防御 [5]，最大化 WAF 的安全增益。其核心在于使 WAF 防护策略从固定规则预配置，演进为能够根据当前的攻击态势、业务负载和威胁情报进行实时权衡和动态调整的智能体系，其过程如图 1 所示。

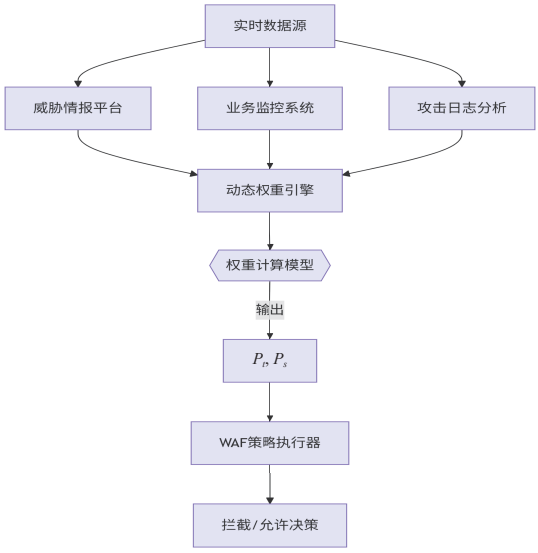

图 1 动态适配机制图

3.1 动态适配模型

3.1.1 模型说明

本模型基于一个基本假设：正常业务访问和恶意攻击行为在时空分布上存在差异性。例如，内部员工访问 OA 系统通常在工作时间段（时间合规）和公司网络内（空间合规）；而一次成功的撞库攻击，其登录请求可能来自陌生地域（空间异常），并在凌晨时段集中爆发（时间异常）。本模型即利用这种差异性，在传统技术规则之外，增加了一层基于业务逻辑的柔性防护，相对于其他基于多源日志 [6]，心智理论入侵响应系统 [7]，三位一体的威胁情报系统 [8] 等网络安全模型，具有轻量级特性，兼顾实时性与可部署性。如表 5 所示。

表 5 动态适配模型

服务器群	策略类型	一级指标	二级指标	权重	主体	变量	取值范围	安全增益
业务系统	动态适配（非技术型审查引擎）	业务属性	时间策略	P_t	客户端	C	WAF 日志时间字段集 $[C_1, C_2]$	拦截 / 允许 / 部分允许
					组织端	T	自定义时间窗口 $[T_1, T_2]$	
			空间策略	P_s	客户端	G	WAF 日志 IP 字段集 $\{G_1, G_2,...,G_i\}$	
					业务对象	O	组织授信 IP 池 $\{O_1,O_2,...,O_i\}$	
					服务器群	W	应用服务器 IP 集合 $\{W_1, W_2,...,W_i\}$	

表 6 多因子权重计算模型

因子类别	因子符号	系数	计算方法	影响方向	更新频率
时间因子					
业务属性系数	α_t	0.3	金融 =1.0，政务 =0.4，默认 =0.7	P_t↑	每日
攻击集中度	β_t	0.4	非工作时间攻击次数 / 总攻击次数	P_t↑	每小时
业务峰值时段	γ_t	0.3	当前时段请求量 / 日均峰值请求量	P_t↓	实时
空间因子					
IP 威胁评分	α_s	0.5	威胁情报平台 IP 信誉评分（0~1）	P_s↑	实时
地理风险指数	β_s	0.3	高风险区域访问次数 / 总访问次数	P_s↑	每 10 分钟
业务敏感度	γ_s	0.2	数据敏感等级（1~5 级分别映射 0.2~1.0）	P_s↑	按需

3.1.2 模型指标与因子解释

业务属性：组织的业务类型，如金融、政务等；客户端访问时间（C）：用户发起请求的时间变量 C，其值的集合为 $[C_1,C_2]$；组织时间（T）：系统服务的时间窗口，其值的集合为 $[T_1,T_2]$；客户端（G）：用户发起请求位置变量 G，其值为 WAF 解析的日志数据“客户端 IP”，属于集合 $\{G_1,G_2,...,G_i\}$；业务对象（O）：自定义变量 O 值为组织授信 IP，属于集合 $\{O_1,O_2,...,O_i\}$，同时支持实时信誉库联动（如威胁情报平台）；权重（P_t、P_s）：分别为时间策略和空间策略的优先级标识。

3.1.3 运作逻辑

（1）访问请求触发。客户端 G（$G\in\{G_1,G_2,...,G_i\}$）在时间 C（$C\in[C_1, C_2]$）时向服务器 W（$W\in\{W_1,W_2,...,W_i\}$）发起请求。

（2）动态策略匹配。动态策略的匹配主要是根据多因子权重计算模型（如表 6 所示）基于外部实时威胁进行自适应调节并输出结果。该模型通过一组可配置的系数 (α, β, γ)，将抽象的“业务属性”“攻击态势”等因素转化为具体的权重值 P_t 和 P_s。其计算过程可简要概括为：

① 因子量化：从日志和外部威胁情报平台实时获取各因子的原始数据（如当前攻击频率、IP 信誉得分等）

② 权重计算：根据公式 $P_t = \alpha_t$ 业务属性 $+\beta_t$ 攻击集中度 $+\gamma_t(1-$业务峰值$)$，$P_s = (\alpha_s$ IP 威胁 $+\beta_s$ 地理风险 $+\gamma_s$ 业务敏感度$)$ 计算出原始权重。

③ 归一化处理：归一化公式为 P_t= 原始 P_t/(原始 P_t+ 原始 P_s)，最终权重需满足 $P_s+P_t = 1$，$0.1 \le P_s$, $P_t \le 0.9$ 的约束条件，以确保决策的一致性。

（3）多因子权重指标解释。业务属性系数：由变量 W 区分业务本质，如金融业务（高 P_t），政务业务（高 P_s）；攻击集中度：当时间窗口 C 外攻击占比高，提升时间权重（强化非工作时间拦截）；业务峰值时段：当处于业务系统高峰期 T 时，自动降低 P_t，减少系统负载；IP 威胁评分：根据组织授信库 O 或威胁情报对来自客户 G 的 IP 进行实时评分；地理风险指数：自动识别高风险地区；业务敏感度：对业务系统的数据等级进行定义。

（4）表 7 为金融业务的多因子权重计算示例。

表 7 多因子权重计算示例

因子	值	计算过程	贡献值
业务类型	1	0.3×1.0	0.30
攻击集中度	0.8	0.4×0.8	0.32
业务峰值	0.9	0.3×(1−0.9)	0.03
原始 P_t		0.30+0.32+0.03	0.65
IP 威胁	0.4	0.5×0.4	0.20
地理风险	0.2	0.3×0.2	0.06
业务敏感度	0.6	0.2×0.6	0.12
原始 P_s		0.20+0.06+0.12	0.38
归一化结果		P_t=0.65/（0.65+0.38）	0.63
		P_s=0.38/（0.65+0.38）	0.37

3.1.4 安全输出

拦截：直接拒绝访问（非工作时间请求或非授信 IP）。

允许：时间和位置都在合规范围内。

部分允许：部分受限访问，如特定时间窗口外仅开放只读权限，以适应一些灰度场景。

3.2 实验及分析

实验数据为真实网络环境下日志，包含多种攻击事件，由于网络安全态势涉及的变量因素多，安全链条长，为了说明动态适配机制，从客户端到服务器端全过程中仅抽取网络安全链上的 WAF 节点所产生安全日志来验证比较基于 WAF 语义规则静态策略和动态适配两种机制下安全增益（如表 8 所示）。

表 8 动态测试结果

单位：%

序号	攻击类型	静态策略（拦截率）	动态适配机制（拦截率）	增益幅度
1	路径遍历攻击	76.60	94.20	17.60
2	系统命令注入攻击	43.00	62.80	19.80
3	SQL 注入攻击	81.30	89.50	8.20
4	Webshell 检测	96.30	98.70	2.40
5	Web 服务器漏洞攻击	96.10	97.20	1.10
6	跨站脚本攻击	91.80	95.20	3.40
7	其他攻击	7.90	53.70	45.80

动态适配机制对各类攻击的拦截率均有提升，平均增幅达 14.3%，其中，对 DIR、OSI、其他攻击的拦截率有大幅提高。相较于静态策略，动态适配机制具有以下优势：一是安全有效性显著提升，通过实时调整权重，对各类攻击的拦截更加精准。例如，系统在检测到大量低频 SQL 注入尝试时，模型自动提升 P_t 值，从而加强了基于时间异常（如凌晨非业务时间窗口）的检测。二是对未知攻击（如远程文件访问尝试、HTTP 请求头部攻击检测）如防御能力质变，这是模型最大价值，面对“其他攻击”，模型能根据 IP 威胁评分和地理风险指数等因子，实时赋予空间权重 P_s，即使无法识别攻击特征，也能因其行为异常（如来自高危地区的 IP 在异常时间访问）而进行拦截，验证了业务规则驱动安全的可行性。

4 结论

本文提出的基于多因子权重计算的动态适配机制，通过把时间维层次的长短周期变量 [9] 与业务属性等日志上下文因素有机结合，构建了一个轻量级的“情景大脑”，使 WAF 从基于技术特征的静态防护，转向基于风险感知的动态智能防御。同时，生成式人工智能对安全攻防两端的双向赋能，正倒逼网络安全展望未来，WAF 的演进也必将与 AI 技术深度融合，重新构建一套具备治理升级迭代 [10]。多维防护能力的智能安全体系架构，且这一体系应具有自适应性、透明度和灵活性的智能规则生成系统 [11]，实现防护策略的动态优化和持续演进。

参考文献：

[1]NIST 大数据公共工作组（NBD-PWG）定义与分类子组 .NIST 大数据定义（草案）[R/OL].2018[2026-05-08]. https://www.nist.gov/publications/nist-big-data-interoperability-framework-volume-1-big-data-definitions-version-2.

[2] 国家互联网应急中心 .2021 年上半年网络安全漏洞态势报告 [R/OL].2021[2026-05-08].https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf.

[3]Check Point Research. Global cyber attack trends : 2022 mid-year report[R/OL].2022[2026-05-08].https://research.checkpoint.com/2022/check-point-softwares-mid-year-security-report-reveals-42-global-increase-in-cyber-attacks-with-ransomware-the-number-one-threat/.

[4] 陈秀真 , 郑庆华 , 管晓宏 , 等 . 层次化网络安全威胁态势量化评估方法 [J]. 软件学报 ,2006,17(4):885-897.

[5] 邬江兴 . 网络空间拟态防御研究 [J]. 信息安全报 , 2016, 1(4):1-10.

[6] 陆雨晶 . 基于多源日志的网络安全威胁感知关键技术研究 [D]. 镇江 : 江苏科技大学 ,2019.

[7] 程秋美 . 智能化网络空间安全态势感知方法及应用研究 [D]. 杭州 : 浙江大学 ,2021.

[8] 陈明 , 高金虎 . 基于威胁情报的网络空间安全态势感知研究 [J]. 情报杂志 ,2024,43(8):25-33.

[9] 王波 . 基于时间维层次化的网络安全态势评估技术研究 [D]. 天津 : 天津理工大学 ,2018.

[10] 桂畅旋 , 杜文越 . 生成式人工智能对网络安全产业影响分析 [J]. 信息安全与通信保密 , 2024(8):11-19.

[11] 耿聪聪 . 基于人工智能的网络安全管理的研究 [D]. 青岛 : 中国石油大学 (华东),2018.

【作者简介】

许俊龙（1981—），男，安徽全椒人，本科，工程师，研究方向：网络安全、网络规划。

徐爱华（1978—），女，江苏南通人，本科，高级工程师，研究方向：系统架构。

王松（1981—），男，江苏南京人，硕士研究生，高级工程师，研究方向：网络安全、网络规划。

（收稿日期：2025-10-16 修回日期：2026-05-13）