让 WAF 专职做好流量清洗工作

2026 年 7 月 13 日

当前，Web 应用防火墙（WAF）已成为网站安全体系中的标配设备。无论是政府门户、金融机构、电商平台，还是大中型企业的官方网站，WAF 几乎是“人手一台”的刚需产品。然而，一个令行业尴尬的现实是：大量安全运维人员反馈，WAF 在实际部署中的防护效果远不如预期，误报频发、性能瓶颈频现、证书更换频繁令团队苦不堪言。有些用户甚至开始质疑：花了十几万甚至几十万采购的 WAF 设备，到底有没有起到应有的作用？

问题出在哪儿？根源不在 WAF 的检测引擎。事实上，主流 WAF 的检测规则库和 AI 语义分析能力已经相当成熟。问题出在 WAF 被赋予了太多“本职工作”之外的任务。

让我们回顾一下互联网安全架构的演变。十年前，HTTP 明文流量占主导，WAF 只需监听 80 端口，对明文流量做七层检测即可。部署简单、职责清晰、效果显著。但今天，全球 HTTPS 流量占比已超过 95%，部分统计甚至显示已达 98%以上。当所有流量都穿上了加密的“铠甲”，WAF 原本清晰的职责边界开始模糊。它不仅要当“安检员”，还要当“开锁匠”，先解密、再检测、再加密回传。更麻烦的是，这把“锁”还在不断升级换代：从 RSA 到 SM2，从混合 PQC 到未来的纯 PQC MTC 证书，每一种新算法的引入都意味着 WAF 设备需要重新适配、升级、测试。与此同时，SSL 证书的有效期从过去的 3-5 年一路缩短到现在的 200 天，明年的 3 个月，2029 年的 1 个半月，甚至将来的一周。这意味着 WAF 设备上的证书每周天就要更换一次，如果全部靠人工操作，WAF 的运维成本将远远超过其采购成本。

三重压力叠加之下，WAF 正在被它不应该承担的任务压垮。本文的核心观点是：**让 WAF 做回 WAF！专业的设备应该只做自己专业的事情。**

一、WAF 的本职是什么？

在讨论“WAF 应该做什么”之前，我们有必要先厘清 WAF 的职责边界。

Web 应用防火墙（Web Application Firewall）的核心职责，是过滤和监测 Web 应用与互联网之间的 HTTP 流量，对流量进行恶意特征识别及防护，在对流量清洗和过滤后，将正常、安全的流量返回给 Web 服务器，防护网站服务器被恶意入侵。

与传统的网络层防火墙（工作在三层或四层）不同，WAF 工作在应用层（第七层）。它能

够深入解析 HTTP 请求的头部、参数、Cookie、请求体等细节，精准识别并拦截 SQL 注入、跨站脚本（XSS）、代码执行、远程文件包含、命令注入等 Web 应用层的攻击行为。现代 WAF 通常采用规则引擎与 AI 语义分析引擎协同工作的方式，实现对恶意流量的智能识别和阻断。

从这个定义中可以清晰地看出：WAF 处理的对象是**明文 HTTP 流量**，WAF 输出的成果是**清洗后的安全流量**。它不负责加密、不负责解密、不负责证书管理，就像机场安检员不需要负责给乘客的行李上锁或开锁一样。

然而，现实中的 WAF 却被迫成为了一名“兼职锁匠”。

二、WAF 正在被三重压力压垮

第一重压力：加密流量的全面覆盖。

HTTPS 的普及无疑是互联网安全的一大进步，但它也给安全检测带来了新难题。WAF 若无法解密 HTTPS 流量，就只能对明文部分（如 HTTP 头部、SNI 信息）进行有限防护，根本无法识别加密内容中隐藏的 SQL 注入、恶意脚本等攻击载荷。更要命的是，根据多家安全厂商的年度报告，目前超过 85%的网络攻击已隐藏在加密流量之中，加密本是保护数据安全的“盾牌”，如今反而成了攻击者的“隐身衣”。WAF 想要看到攻击，就必须先解密；而解密，从来不是 WAF 的设计强项，更不是安全厂商的技术强项。

第二重压力：密码算法的持续多元化。

过去二十年，WAF 设备只需要处理 RSA 一种密码体系的 HTTPS 流量。但今天的情况已经完全不同。国密 SM2 算法已在政务、金融等关键信息基础设施领域广泛部署，并将继续发展到普及的地位，任何要服务这些行业的 WAF 都必须支持国密解密。更前沿的是，后量子密码（PQC）迁移已进入倒计时，从目前的趋势来看，PQC 的部署路径大致分为三个阶段：先以“传统算法+PQC 算法”混合模式过渡，未来再过渡到纯 PQC 算法的 MTC 证书。这意味着 WAF 设备不仅要支持 RSA 解密，还要支持 SM2 解密，还要支持混合 PQC 解密，未来还要支持纯 PQC 解密。这对 WAF 设备的密码运算能力和算法适配能力（需要持续升级软件）提出了指数级的要求。

第三重压力：证书有效期的不断缩短。

如果说算法多元化是“质量”上的挑战，那么证书有效期缩短就是“频率”上的折磨。SSL 证书的有效期从上个世纪的三到五年，缩短到一年，再到现在的半年，2027 年缩短为 3 个月，2029 年为 1 个半月，最终缩短为 1 周。这意味着从 2027 年开始，WAF 设备上部署的 SSL 证书每隔 3 个月就要更换一次。如果 WAF 本身承担证书管理职责，运维团队将陷入无休止的证

书申请、部署、续期、验证的循环之中，这种重复性劳动不仅消耗人力，更增加了因证书过期导致 WAF 防护功能中断的风险。

三重压力叠加之下，WAF 设备如果既要负责 HTTPS 解密，又要负责证书管理，还要负责流量清洗，其结果必然是“样样通、样样松”，解密性能下降、证书管理混乱、清洗效率打折。一个本该专注于安全检测的设备，被活生生逼成了“全能打杂工”。

三、解耦：前置部署 SSL 卸载网关

解决上述困境的思路其实并不复杂：**解耦**。将“HTTPS 解密与证书管理”和“流量清洗”这两个职责分离，让专业的设备做专业的事。

最佳实践是在 WAF 设备之前部署一台 SSL 卸载网关（如零信国密 HTTPS 加密自动化网关）。这台前置网关专职负责：

一是证书自动化。 网关内置自动化证书管理能力，自动对接 CA 系统完成双算法 SSL 证书的申请、验证、部署和续期。无论证书有效期缩短到 3 个月还是 1 周，对运维团队来说都是“透明”的，网关会自动处理一切，无需人工干预。自动化 ACME 协议的支持让这一切变得像呼吸一样自然。

二是 HTTPS 卸载。 网关集中处理 SSL/TLS 加解密，将加密流量解密为明文 HTTP 流量后转发给后端的 WAF 设备。网关内置高性能硬件密码卡，支持 RSA、ECC、SM2 国密乃至混合 PQC 等多种密码算法。无论密码体系如何演进，只需升级网关即可，WAF 设备无需任何改动。

三是协议转换。 网关完成 HTTP 到 HTTPS 的协议转换、RSA 到 SM2 的算法转换、IPv4 到 IPv6 的地址转换等多重转换工作，成为前端与后端之间的“翻译官”。

经过前置网关卸载后的流量是明文的 HTTP 流量，这正是 WAF 最擅长处理的“原材料”。WAF 设备不再需要关心证书从哪来、用什么算法、什么时候过期，只需专注于自己的本职工作：对明文流量进行深度检测、恶意特征识别和流量清洗。这才是 WAF 应有的工作状态。

零信技术实践： 零信国密 HTTPS 加密自动化网关不仅全面支持 RSA 密码体系、SM2 国密体系和混合 PQC 算法，实现高效的 HTTPS 卸载，而且其自身内置了 A 级 WAF 一体化能力。需要强调的是，内置 WAF 的定位并非取代用户已有的专业 WAF，而是作为一种**灵活的补充方案**：对于尚未采购 WAF 的单位，网关内置的 WAF 能力可以提供开箱即用的安全防护；而对于已部署专业 WAF 的用户，完全可以选择关闭自动化网关的内置 WAF 功能，由网关专职做 SSL 卸载，将明文流量直接转发给后端的专业 WAF 清洗。

四、各司其职，才是正解

让 WAF 做回 WAF，只负责流量清洗，把加密和证书的事交给 SSL 卸载网关。这是应对 HTTPS 全面普及、密码算法多元化和证书有效期不断缩短的正确架构选择。

SSL 卸载网关做 SSL 卸载的事，WAF 做流量清洗的事，各司其职、各展所长。加密环境再复杂、算法演进再快、证书有效期再短，只要两种不同功能的设备各司其职，用户的安全投资就永远不会过时。

更重要的是，这种架构保护了用户的既有投资。很多用户已经采购了功能强大的专业 WAF 设备，不要因为无法支持新密码算法或无法实现证书自动化而被闲置或替换。通过增加 SSL 卸载网关，这些 WAF 设备可以“重获新生”，继续发挥其最擅长的流量清洗能力。这才是对用户投资最大的尊重。

专业的人做专业的事，专业的设备干专业的活。

王高华

2026 年 7 月 13 日于深圳
