数字认证

ssl.bjca.cn

数字认证 SSL自动化网关内置WAF性能测试报告

2026年4月8日

一 概述

Web应用防火墙（WAF）是保障网站安全的核心组件，用于抵御SQL注入、跨站脚本（XSS）、命令注入等各类Web攻击，同时也是等保2.0、密评等合规要求的必备能力。

数字认证 SSL自动化网关内置企业级WAF模块，经国际权威机构**Cloudbric** WAF性能在线测试系统WAFER实测，防护性能达到**最高A级**。更重要的是，网关采用**一体化架构**，将HTTPS加密卸载与WAF清洗合二为一，从根本上解决了传统WAF因证书过期而失效的致命问题，实现“一次部署、5年无忧”的安全防护。

二 WAF核心性能指标：真阳、假阴、假阳、真阴

衡量WAF性能需理解四个国际通用的核心指标：

指标	英文术语	含义	安全影响
真阳	**True Positive**	成功拦截攻击流量	正确防护，应保持高比例
假阴	**False Negative**	漏拦攻击流量（最危险）	攻击者绕过WAF，需极力避免
假阳	**False Positive**	误拦正常流量（次危险）	影响正常业务访问，需极低比例
真阴	**True Negative**	正确放行正常流量	理想状态，由假阳率推算

最理想状态：假阴 = 0，假阳 = 0，真阳率 = 100%。

三 数字认证 SSL自动化网关WAF性能测试结果（Cloudbric WAFER权威测试）

本报告引用**Cloudbric WAFER**（国际权威WAF测试平台）的实测数据。

◆ **测试网址：**https://labs.cloudbric.com/wafer

◆ **测试对象：**数字认证 SSL自动化网关WAF保护的网站（https://gwtest.****.net）

◆ **测试时间：**2026年4月8日

3.1 综合性能评级

指标	测试结果	等级
检测能力（Detection Ability）	**A级**	最高等级
识别能力（Distinguishing Ability）	**A级**	最高等级
真阳率（攻击拦截率）	**98.06%**	远超A级门槛（≥95%）
假阳率（正常流量误拦率）	**0%**	完美，无错误拦截
假阴率（攻击漏拦率）	**1.94%**	极低，持续优化中

测试数据原文：

True Positives: 413 requests, 405 detected, **98.06**%

False Positives: 72 requests, 0 detected, **0%**

3.2 各类攻击拦截详情

攻击类型	攻击次数	拦截次数（真阳）	漏拦次数（假阴）	拦截率
SQL注入	128	126	2	**98.44%**
跨站脚本（XSS）	149	147	2	**98.66%**
命令注入	41	40	1	**97.56%**
服务器端包含注入（SSI）	24	24	0	**100%**
文件上传	29	29	0	**100%**
目录遍历	20	17	3	**85.00%**
缓冲区溢出	10	10	0	**100%**
本地文件包含（LFI）	10	10	0	**100%**
远程文件包含（RFI）	2	2	0	**100%**
总计	**413**	**405**	**8**	**98.06%**

数据来源：Cloudbric WAFER在线测试报告。

3.3 无WAF防护的对比测试

为直观展示WAF的价值，测试工程师同时对**没有WAF防护的网站**进行了相同测试，结果如下：

攻击类型	拦截率
SQL注入	**0%**
跨站脚本（XSS）	**0%**
命令注入	**0%**
服务器端包含注入	**0%**

结论：无WAF防护的网站，所有攻击均可成功实施，网站完全暴露在威胁之下。这就是所有没有WAF防护的网站的真实安全状况。

四 数字认证 SSL自动化网关内置WAF的独家优势：一体化架构彻底解决证书过期问题

4.1 传统WAF的致命缺陷：证书管理与WAF分离

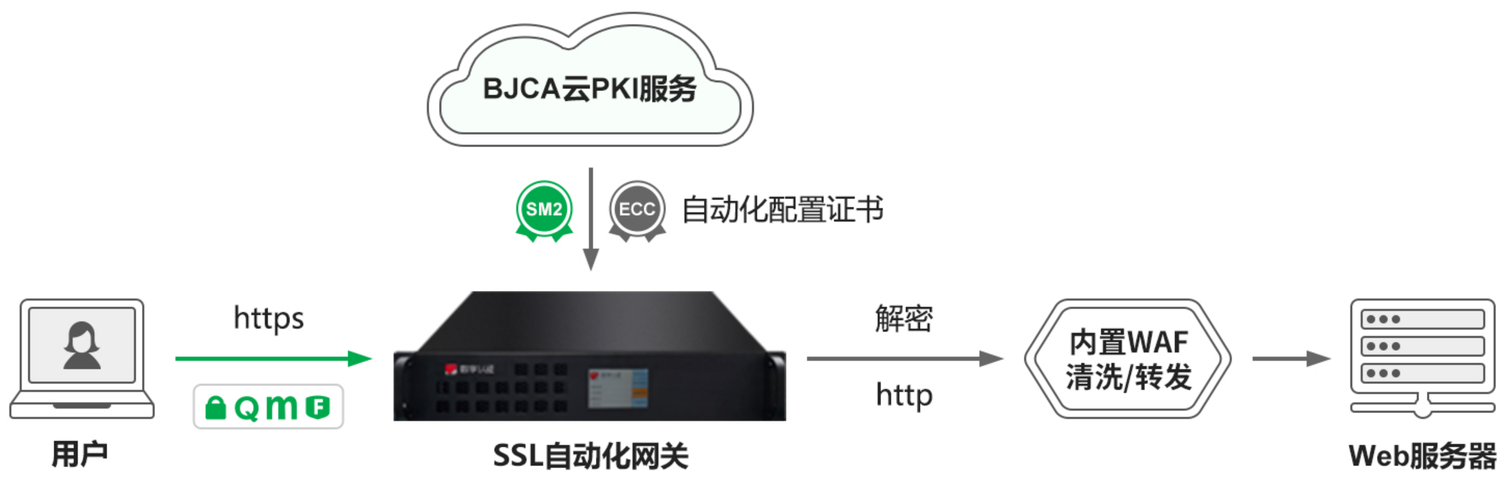
传统WAF设备或云WAF服务的工作原理如下(假设已支持国密)：

传统WAF需要**自行处理HTTPS加密流量**，因此必须持有被防护网站的有效SSL证书。这带来四大问题：

问题	后果
证书有效期缩短	证书有效期将不断缩短至100天、47天，人工导入证书频率剧增
国密算法支持	必须支持国密SSL证书和国密算法HTTPS加密
操作遗漏风险	一旦忘记导入证书，则不仅浏览器访问提示证书错误，而且WAF无法解密HTTPS，只能降级为保护HTTP明文，防护归零
运维负担重	几十个甚至成百上千个网站的WAF防护需逐一人工导入SSL证书，极极易出错

4.2 数字认证 SSL自动化网关的解决方案：一体化架构，WAF系统无需接触证书

数字认证 SSL自动化网关采用**一体化架构**，将HTTPS加密卸载与WAF清洗合二为一：



关键差异：

对比项	传统独立WAF	数字认证网关一体化架构
证书持有者	WAF自身	**网关的证书自动化系统**
WAF是否接触证书	是，需持有证书	**否，只处理解密后的HTTP流量**
证书过期影响	WAF失效	**无影响（网关自动续证书）**
证书导入方式	人工导入	**自动配置/自动续期**
运维负担	每年至少4-10次人工操作	**5年零运维**

4.3 为何一体化架构彻底解决WAF证书过期问题？

传统架构的死循环：

(1) 网站SSL证书有效期不断缩短
(2) WAF需要人工同步导入私钥和证书
(3) 一旦遗漏导入，WAF失效
(4) 无法解密的WAF只能降级为保护HTTP明文 → 防护归零

数字认证网关的破解之道：

(1) 网关内置**证书自动化系统**，自动为网站配置/续期证书
(2) 网关在入口处完成HTTPS解密，将明文HTTP流量交给WAF
(3) **WAF模块无需持有证书**，永远不面临证书过期问题
(4) 证书自动化与WAF清洗在同一个设备内完成，**天然联动，无需人工同步**

一句话总结：传统WAF的证书问题是“架构性”的——因为它必须自己持有证书；而数字认证网关的WAF是“架构性”的解决方案——证书管理在网关入口完成，WAF只处理明文，从根本上消除了证书过期的风险。

五 WAF防护等级说明

5.1 等级划分（Cloudbric标准）

等级	真阳率	说明
A级	≥95%	优秀，可拦截绝大多数攻击
B级	85%–94%	良好，可拦截大部分攻击
C级	70%–84%	合格，可拦截主要攻击
D级	<70%	不合格，不建议使用

5.2 数字认证网关WAF评级

根据Cloudbric WAFER权威在线测试报告：

维度	评级
检测能力（Detection Ability）	**A级**
识别能力（Distinguishing Ability）	**A级**
真阳率	**98.06%**（远超A级门槛）
假阳率	**0%**（完美）
覆盖攻击类型	SQL注入、XSS、命令注入、SSI注入、文件上传、目录遍历、缓冲区溢出、LFI、RFI等OWASP Top 10主要威胁

综合评级：A级（最高等级）

六 部署建议：WAF + 证书自动化 = 真正的安全防护

6.1 单独部署WAF的风险

如果仅部署WAF而不实现证书自动化，将面临：

- ◆ **证书过期导致WAF失效：**每年至少4-10次人工操作，一旦遗漏，防护归零
- ◆ **国密改造无法落地：**传统WAF设备或者云WAF服务通常不支持国密SSL证书和国密算法，无法满足等保和密评要求
- ◆ **运维成本高企：**大量网站的证书管理+WAF证书导入，至少需要1-2名专职人员

6.2 一体化方案的价值

数字认证 SSL自动化网关将**证书自动化 + 国密改造 + 后量子加密 + A级WAF**整合为一体：

- ◆ **一次部署：**网关并行或前置接入，无需改造网站架构
- ◆ **5年无忧：**证书自动续期、WAF天然集成，全程零运维
- ◆ **双重合规：**同时满足等保2.0和密评GM/T 0054要求
- ◆ **三重防护：**Web攻击防护 + 传统HTTPS加密 + 后量子密码HTTPS加密

七 总结

维度	结论
测试系统	Cloudbric WAFER（国际权威）在线实时测试
测试结果	**A级**，真阳率98.06%，假阳率0%
核心优势	**一体化高效架构**，先HTTPS加密卸载，紧接着就是流量清洗。WAF无需持有证书，彻底消除证书过期风险
覆盖攻击	SQL注入、XSS、命令注入、SSI注入、文件上传、目录遍历、缓冲区溢出、LFI、RFI等OWASP Top 10主要威胁
部署方式	前置或并行部署，无需改造网站架构
运维成本	5年零运维，彻底解放运维工程师

数字认证 SSL自动化网关不仅是证书自动化管理设备，更是集A级WAF防护于一体的网站安全全能方案。选择数字认证网关，您将同时获得：

- ◆ 证书全生命周期自动化（多CA高可用）
- ◆ 国密改造一键完成
- ◆ 双混合PQC加密
- ◆ **A级WAF防护（Cloudbric权威认证），一体化架构，永不过期**

一台设备，解决网站加密与防护的全部核心问题。 数字认证网关内置A级WAF，一体化架构，防护永不过期

本报告基于Cloudbric WAFER权威测试数据。如需测试报告原文，进一步了解技术细节或获取演示支持，请联系数字认证技术支持团队。

北京数字认证股份有限公司 国有控股上市企业（300579） · 北京数据集团核心成员 · 数字认证，SSL证书自动化领导者

联系我们：官网 ssl.bjca.cn 服务热线 4009-197-888 邮箱 ssl@bjca.org.cn