传统SSL网关替代方案对比

数字认证 SSL自动化网关 vs. 传统SSL网关

一 为什么要替代传统SSL网关?

传统SSL网关在过去十年中，主要承担SSL/TLS卸载、负载均衡等职能。然而，随着网站HTTPS加密环境的深刻变化，传统SSL网关的局限性日益凸显：

趋势	对传统SSL网关的挑战
证书有效期缩短	200天→100天→47天，人工导入网关的证书管理已不可能
国密合规强制	传统SSL网关如果不支持国密算法，无法通过密评。部分网关虽支持国密，但仅支持TLS 1.2，**不支持TLS 1.3国密算法，且不具备前向安全性**。
后量子威胁现实化	传统网关不支持后量子密码，数据面临“先收集后解密”风险
WAF成为刚需	传统网关无WAF功能，需额外采购、集成、管理

结论：传统SSL网关已无法满足当前和未来的网站安全需求。替代方案必须具备**证书自动化、TLS 1.3国密支持（含前向安全）、后量子密码就绪、内置WAF**四大能力。

二 核心对比：一张表看懂差异

对比维度	传统SSL网关	数字认证 SSL自动化网关
证书管理方式	**人工管理：**需手动导入私钥和证书、续期证书	**全自动：**自动申请、自动部署、自动续期，5年零运维
证书有效期适应能力	**无法适应：**有效期越短，人工负担越重	**天然适应：**证书越短，自动化价值越大，支持每天更新证书
多CA高可用	不支持	**支持：**对接多家国际CA+国密CA，毫秒级自动切换
国密算法支持	不支持或仅支持TLS1.2	**原生支持TLS 1.3国密算法：**自动配置国密证书，一键完成国密改造
前向安全 (Forward Secrecy)	不支持	**支持：即使证书私钥泄露，历史加密数据也无法被解密。**独家同时支持国际算法和国密算法TLS 1.3
后量子密码（PQC）	不支持	**全球独家支持：**SM2MLKEM768 + X25519MLKEM768双混合PQC算法
WAF功能	无，需单独采购	**内置A级WAF**（Cloudbric权威认证，真阳率97.34%，假阳率0%）
WAF证书联动	不适用（WAF需单独导入证书）	**一体化架构：**WAF无需持有证书，永不面临过期问题
部署方式	旁路部署	旁路部署，无需改造网站架构
运维负担	高：每年多次人工操作	低：5年零运维
业务连续性风险	高：证书过期导致业务中断	无：证书自动续期，业务永远在线
总拥有成本（5年）	网关采购费 + 证书费 + WAF采购费 + 人力成本	网关采购费（含5年证书 + 内置WAF）

三 深度解析：为什么数字认证网关是更好的选择？

3.1 证书自动化：从“人工负担”到“零运维”

传统SSL网关：

◆ 证书有效期缩短趋势下，每年需人工操作2次、4次、8次
◆ 200个网站 = 每年400次、800次、1600次人工操作
◆ 一次遗漏，业务中断

数字认证网关：

◆ 自动对接多家CA，自动申请、自动续期、自动部署
◆ 管理员只需配置一次，5年内无需任何人工干预
◆ **证书有效期越短，自动化价值越大**

3.2 国密支持：从“无法合规”到“一键完成”

传统SSL网关：

◆ 通常不支持国密算法
◆ 如需满足密评要求，需额外部署国密专用设备，增加架构复杂度

数字认证网关：

◆ 原生支持国密SM2算法，率先支持国密TLS1.3，支持前向安全
◆ 自动签发国密OV证书，自动部署
◆ **一键完成国密改造，满足等保2.0、密评GM/T 0054要求**

3.3 后量子密码：从“未来威胁”到“当下防护”

传统SSL网关：

◆ 不支持后量子密码
◆ 网站数据面临“先收集、后解密”的现实威胁

数字认证网关：

◆ **全球独家支持双混合PQC算法：**SM2MLKEM768（中国方案）+ X25519MLKEM768（国际方案）
◆ 部署后所有网站即刻获得后量子加密能力
◆ 与**零信浏览器**配套，实现端到端后量子密码HTTPS加密生态

3.4 WAF功能：从“额外采购”到“一体化集成”

传统SSL网关：

◆ 无WAF功能，需单独采购WAF设备或云服务
◆ 额外采购意味着：单独预算、单独部署、单独管理
◆ 更严重的是：**WAF需要人工导入证书**，证书过期则WAF失效，业务中断

数字认证网关：

◆ 内置A级WAF，无需额外采购
◆ **一体化架构：**网关先完成HTTPS解密，WAF只处理明文流量，**WAF无需持有证书，永不面临过期问题**
◆ Cloudbric WAFER权威在线测试：**真阳率98.06%，假阳率0%，检测能力和识别能力均为A级**

四 替代价值计算：5年总拥有成本对比

假设场景：200个网站，5年周期

成本项	传统SSL网关方案	数字认证网关方案
SSL网关设备（5年折旧）	20万元	**包含在网关中**
SSL证书费用（200个网站×5年）	按100天有效期，至少需4次申请通配证书 → 约5万元	**5年证书已包含**
WAF设备（5年折旧）	20万元	**包含在网关中**
WAF证书管理人力	1人×5年 = 约60万元	**0元**
总计	**约105万元**	**约40万元（网关采购价）**

数字认证网关节省成本约65万元，同时消除了证书过期导致业务中断的风险。

五 替代路径：如何平滑迁移？

步骤	操作	说明
1. 评估现状	梳理现有网站数量、证书管理方式、WAF使用情况	数字认证销售/售前可协助
2. 部署网关	旁路接入，无需改造网站架构	1小时内完成部署
3. 切换流量	将网站流量指向网关	可分批切换，降低风险
4. 验证运行	确认证书自动签发、WAF正常防护	数字认证提供7×24小时支持
5. 下线旧设备	证书全部迁移后，停用传统SSL网关和独立WAF	完成替代

六 总结：为什么选择数字认证网关替代传统SSL网关？

您的需求	传统SSL网关	数字认证网关
证书管理不费力	✗ 人工导入，负担重	✓ 全自动，5年零运维
满足国密合规	✗ 通常不支持	✓ 一键完成国密改造
防御后量子威胁	✗ 不支持	✓ 独家双混合PQC算法
无需额外采购WAF	✗ 需单独采购	✓ 内置A级WAF
WAF永不因证书过期失效	✗ 需人工导入证书	✓ 一体化架构，WAF不碰证书
降低总拥有成本	✗ 需采购多台设备	✓ 一台设备解决全部需求

数字认证 SSL自动化网关，不仅是传统SSL网关的替代者，更是面向未来的网站安全基础设施。它将证书自动化、国密改造、后量子密码加密、A级WAF融为一体，帮助政府、银行、高校、医院等网站密集型机构，以更低的成本、更高的安全性、更少的运维负担，迎接证书有效期缩短和量子时代的安全挑战。

替代传统，一步到位。　数字认证·SSL自动化网关

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