零信网关特色之三：超值-WAF 防护

笔者在《零信网关特色之一：自动化》解读了零信网关同其他网关的最大的不同是“自动化”，这是一个端云一体自动化实现国密 HTTPS 加密的创新解决方案。在《零信网关特色之二：超值-双 SSL 证书》解读了零信网关的超值—5 年免费为最多 255 个网站自动化配置双 SSL 证书，证书价值高达 623 万元。虽然笔者在文章中给出了计算公式，但是有些读者还是有些质疑，因为这在传统的商业产品中的确有些不可思议，可能会让用户认为是夸大宣传，笔者在解读第三个特色之前补充解读一下特色之二的超值。

传统商业产品如果销售价为 38 万元，宣传免费赠送高达 623 万元的附加产品，这的确让人难以置信，第一反应是商家夸大宣传。但是，对于零信网关自动化配置的双 SSL 证书，这是一个数字产品，在密码基础设施投资后的用户量上来后的边界成本可以降得非常低，甚至可以做到完全免费，这就是为何全球第一大 CA – Let’s Encrypt 完全免费自动化提供 90 天 RSA 算法 DV SSL 证书。“自动化”是关键，零信网关就是做到了自动化配置证书，才能把证书价格降了下来，把国密改造成本降了下来，才能实现自动化配置国密算法 OV SSL 证书，实现超值配置证书。按照标配网关售价 38 万元计算，分摊到每个网站的双 SSL 证书费用仅为 298 元/年(=380000 / 255 / 5)，大家可以去网上搜索一下是否有公司提供这么便宜的双 SSL 证书(一张一年期 SM2 OV SSL 证书和一张一年期 RSA DV SSL 证书)，这就是自动化给用户带来的超值！证签官网这样配置的双 SSL 证书就是 OV SSL 证书精简版，销售价格为 4888 元，乘以 255 再乘以 5 就是实打实的 623.22 万元！这是超值之一：节省证书费用。

其实，零信网关给用户带来的超值还不止这个，笔者在第一篇文章就已经列出了自动化给用户带来的节省工程师人力成本的价值，高达 150 万元(=1.25 * 2 * 12 * 5)，255 个网站的 SSL 证书的部署和维护工作需要两个工程师，按照每个运维工程师每月 1.25 万元人力成本计算(包括工资、福利、公司运营成本分摊等)。这些完全可以由机器来完成的工作，并且还不会出错，为何一定要耗费在宝贵的工程师身上呢？应该让工程师去干更重要的工作！上面这个人力成本的节省还是按照目前 SSL 证书有效期为一年来计算的，每 11 个月就要实施一次，而如果证书有效期缩短到了 90 天，每年就要申请和安装证书 5 次，工程师的数量就要增加 5 倍才能完成任务，这就意味着零信网关可以节省 5 * 150 万元 ＝750 万元的人力成本，这就是自动化的厉害，大家也不能理解为何自动化工厂在不断普及的原因了，节省太多人力成本了，而且还不会出错。这是超值之二：节省人力费用。

大家别以为笔者的文章跑题了，前面只是今天本文的引言部分，先给大家总结一下零信网关的前两个超值：节省证书费用和节省人力费用。还有一个超值今天接着讲。

WAF 是 Web 应用防火墙的简称，对网站安全很重要，相信大多数本文读者都知道。笔者在 2022 年写的文章《未来 2 年，70%用户将选择云 WAF 防护》引用 Gartner 的 2021 年报告预测数据：到 2024 年，70%的组织为 Web 应用选用云 WAF 防护。笔者粗略统计了一下欧美的政府网站和大企业网站，这个预测数据是准确的。在我国，各大单位都已经开始采购或者已经采购 WAF 设备，或者正在使用云 WAF 服务，中国政府网 www.gov.cn 已经采用了云 WAF 防护，31 个省市政府官网有 6 个已经启用云 WAF 防护，可能还有些是本地 WAF 设备防护，笔者无法统计到，据了解各种政务云平台都在采购 WAF 设备。

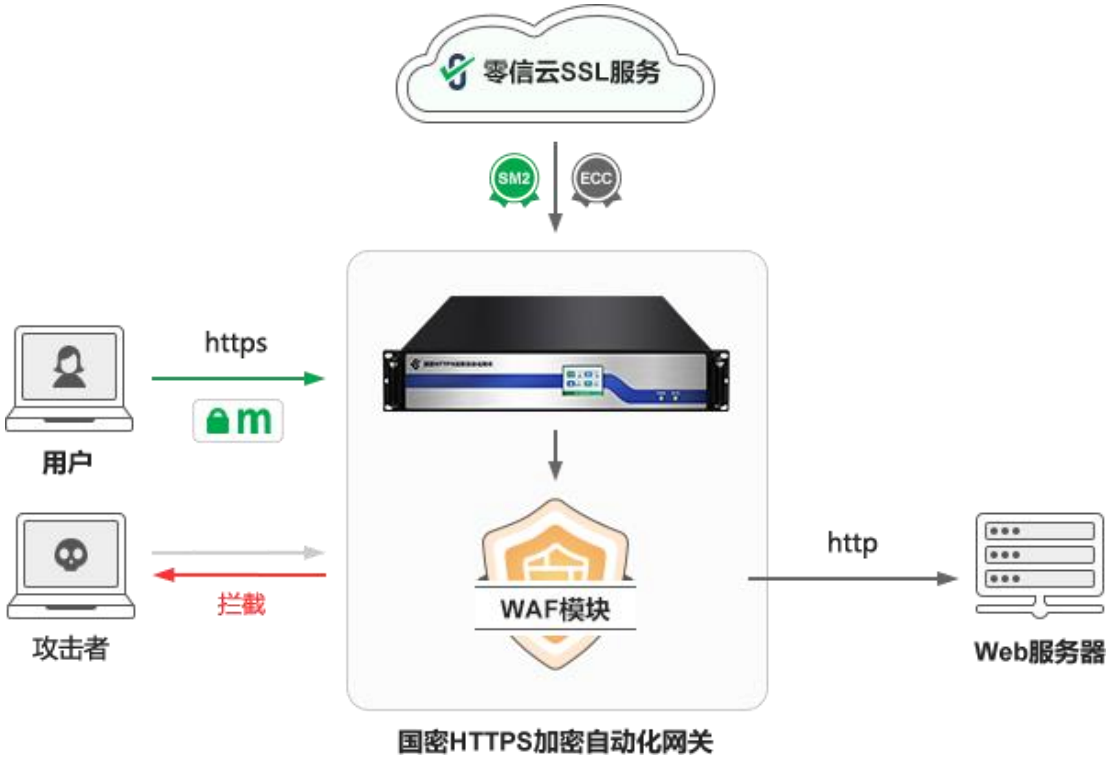
无论是 WAF 设备还是云 WAF 服务，都是在原 Web 服务器之前增加一个 Web 流量清洗服务，拦截恶意连接和放行正常连接。而对于 HTTPS 加密的普及强制应用，WAF 设备和云 WAF 服务就得支持 HTTPS 加密流量的卸载后再清洗。而对于国密合规要求，WAF 设备和云 WAF 服务就得支持国密 HTTPS 加密。卸载国密加密流量后再清洗。这就对 WAF 设备和云 WAF 服务提供了更高的要求。而传统的工作方式是用户向 CA 申请 SSL 证书，再配置到 WAF 设备或云 WAF 服务中去，手动方式费时费力费钱，现在是一年一次，如果 SSL 证书有效期缩短为 90 天，一年就要折腾 5 次。用户购买 WAF 设备或云 WAF 服务的费用一定还会增长，因为需要更多的人力支援提供服务。

熟悉零信网关或者读过前两篇解读零信网关特色的文章的读者一定了解，零信网关在用户 Web 服务器中的部署方式同上面的 WAF 设备部署方式一样，零信网关就是负责卸载 HTTPS 加密流量转发给后面的 Web 服务器。如果用户已经购买了 WAF 设备，则需要在 WAF 设备之

前部署零信网关，让零信网关来自动化完成 HTTPS 加密和卸载，把明文数据转发给 WAF 设备来拦截恶意流量。这样，原先手工申请 SSL 证书，人工部署 SSL 证书的工作就可以交给零信网关来自动化完成了，原 WAF 网关就可以专用于 WAF 防护。

为了减轻用户的 Web 安全防护费用，零信网关集成了基于开源 ModSecurity 的 WAF 系统，默认免费为网关用户提供 WAF 防护服务，这样，还没有采购 WAF 设备的用户就不用增加投资预算去另外采购 WAF 设备了，为用户提供一站式 HTTPS 加密自动化 ＋WAF 防护服务。这就是今天要讲了第三个超值：节省 WAF 设备费用。

零信网关自动化为网站配置双 SSL 证书，自动化实现国密 HTTPS 加密、卸载，由 WAF 模块自动化分析卸载后 Web 流量，拦截恶意流量和放行正常流量到后面的 Web 服务器。一台网关设备内自动化完成 SSL 证书申请、部署、HTTPS 卸载、WAF 防护等全面的网站安全服务，这就是零信国密 HTTPS 加密自动化网关的技术特色。



零信网关这个 WAF 模块的防护性能如何呢？我们用业界有名的 CloudbricLabs 提供的 WAF 性能在线测试工具 WAFER 实测的结果是：检测能力为 B，识别能力为 A。

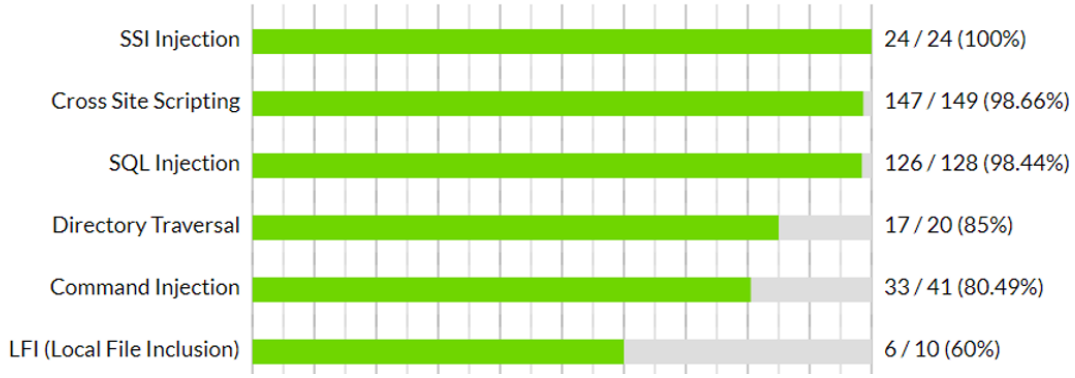
WAFER Report

Type	Total Requests	Detected	Error	%
True Positives	413	354	0	85.71%
False Positives	72	0	0	0%

Performance Scores

Detection Ability	Distinguishing Ability
B	A

具体拦截指标有：100%拦截服务器端包含注入、98.66%拦截跨站脚本攻击、98.44%拦截 SQL 注入、85%拦截目录遍历攻击、80.49%拦截命令注入攻击、60%拦截本地文件包含攻击。笔者把这些指标给一个用户看时，这个用户提出了可能所有用户都会提出的问题：还有未被拦截的攻击怎么办？这的确是一个好问题，笔者的回答是：所有 WAF 都不可能拦截所有攻击，只能是发现了没有拦截的攻击，通过分析攻击来增加防护规则，从而不断增强拦截能力，这是需要用户参与的 WAF 防护日程管理工作。



对于零信网关免费配套的 WAF 防护模块能有这么高的防护性能，笔者还是很欣慰的，这个防护性能相当于买零信网关又免费赠送了一台价值百万的 WAF 设备，因为市场上的售价百万的 WAF 设备的拦截效果也只有这个水平，甚至有些还不如这个水平。不仅如此，目前市场上的所有 WAF 设备都需要用户向 CA 申请和再花钱购买 SSL 证书，都需要人工费时费力部署 SSL 证书，零信网关 WAF 不需要，自动化完成，并且是免费配套 SSL 证书！还有大量的 WAF

设备不支持国密算法和国密 SSL 证书，零信网关 WAF 支持，并且是自动化支持！这些独一无二的价值就是零信网关给用户带来的第三个超值：节省 WAF 设备费用。

为了让用户直观地体验到零信网关 WAF 给用户带来的 WAF 防护价值，零信浏览器特别把零信网关 WAF 也列入了云 WAF 服务提供商数据库，可以像使用了其他云 WAF 服务的网站一样一样明确告诉用户这个网站由零信网关 WAF 提供安全防护，后面的小括号信息是防护节点的编号(sz 代表深圳，后面的 1 代表第一个节点，- 后面的 2 代表第 2 台零信网关)。随着零信国密 HTTPS 加密自动化云服务节点的不断开通，用户会看到更多的不同城市节点的编号。

最后总结一下，零信网关的第三个特色是集成 WAF 模块，为用户网站提供高质量的 WAF 防护。同传统 WAF 设备不同的是，用户无需向 CA 申请和购买 SSL 证书，无需人工手动在 WAF 设备上部署 SSL 证书，这些工作都已经由零信网关自动化免费完成，自动化实现国密 HTTPS 加密、卸载、WAF 防护，把清洗后的干净流量转发给后面的 Web 服务器，让原 Web 服务器零改造完成国密 HTTPS 加密改造，完成 WAF 防护，保障 Web 服务器能不间断地安全加密地为用户提供 Web 服务。

有诗为证：

网站要防护，网站要加密。
零信网关，自动化双提供。
零信网关，超值安全防护。
网站安全，超值双重保障。

王高华

2024 年 3 月 11 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。

已累计发表中文 154 篇(共 40 万多字)和英文 60 篇(7 万多单词)。