ACME vs CWAF

先解释一下标题用的两个英文名称，“**ACME**”是 Automated Certificate Management Environment (自动证书管理环境)的缩写，是一个 RFC 8555 国际标准，用于自动化获取 SSL 证书和自动化部署 SSL 证书，包括 ACME 客户端和 CA 服务端的相关协议标准。“**CWAF**”是 Cloud Web Application Firewall (云 Web 应用防火墙 或 云 WAF)的缩写，是一种云服务，用于对网站或者 APP 的业务流量进行恶意特征识别及防护，将正常和安全的流量回源到 Web 服务器，拦截恶意攻击流量。

今天，零信网站安全云服务上线，特撰文讲讲我们是如何选择技术路线的：ACME 或 CWAF？公司原先的产品研发计划是提供基于 ACME 国际标准的为用户提供全自动部署 SSL 证书的 https 加密服务，但是今天上线的产品并不是这个解决方案，而是基于云 WAF 服务提供的全自动部署 SSL 证书的 https 加密服务，为何有这个研发方向的大改变，本文披露更多的内幕详情。

为了保障证签官网的证书申请与管理系统的安全，我们在官网上线时就选用了阿里云 WAF 服务来保护官网安全，不用不知道，用了才知道，有了云 WAF 服务不仅可以保障网站的安全，而且还可以实现 https 加密服务。这就让我不得不重新思考一个重要的问题：用户还需要 ACME 式的自动获取 SSL 证书服务？我们是否还有必要研发 ACME 客户端和研发对接 ACME 客户端的 SSL 证书签发系统？今天上线的零信网站安全云服务已经给出了答案，这是我公司自己作为一个云 WAF 用户的明智选择，也成为了我公司计划提供的 https 加密服务的技术路线的必然选择。

大家都知道，所有浏览器都已经对没有部署 SSL 证书的网站显示为“不安全”，这不是浏览器厂商吓唬人，是真的不安全，因为 http 是明文传输，如果不采用 https 加密传输，则用户

在网站上输入的所有机密信息都非常容易被非法窃取和非法篡改。而要实现 https 加密，必须向 CA 购买和申请 SSL 证书，好不容易拿到 SSL 证书后还要在服务器上安装和配置使用 SSL 证书才能实现 https 加密，浏览器才会不显示“不安全”，而是显示安全锁标识。

申请和部署 SSL 证书是一件比较痛苦的事情，笔者陪着广大用户痛苦了 18 年之久，所以一直就想为用户提供一个能减轻痛苦的解决方案。所幸的是，市场上已经有了完全免费的能自动化申请和部署 SSL 证书的服务-Let’s Encrypt，这个免费 SSL 证书服务仅用了 6 年时间就赢得了全球 SSL 证书市场 60%的市场份额，遥遥领先其他 CA，已经为全球用户(当然包括中国用户)签发了 4.43 亿张 SSL 证书，其成功的秘诀就是用户只需在服务器上安装一个 ACME 客户端软件就可以全自动获取 Let’s Encrypt 签发的完全免费的有效期为 90 天的 DV SSL 证书。为何 Let’s Encrypt 这么火，因为用户需要简单省事的解决方案，当然最好是免费的。所以，其他 CA 也已经开始支持 ACME 协议为用户全自动提供 SSL 证书，我原先也是这么计划的。

但是，当我们使用了阿里云 WAF 后，我就果断地终止了原先的研发计划，改成了基于云 WAF 服务实现全自动 https 加密，这个方案比 ACME 更简单，更方便，不需要在服务器上安装任何客户端软件，只需做两次 CNAME 域名解析即可！我们把云密码服务的全自动申请 SSL 证书的功能(云 SSL 服务)集成到阿里云 WAF 中， 实现了全自动为阿里云 WAF 配置 SSL 证书，这样就在阿里云 WAF 基础上实现了全自动 https 加密，不同的技术路线一样实现了我们既定的要实现的目标，并且更简单，更先进，同时实现 https 加密和网站安全防护，因为仅有 https 加密并不能保障网站的安全。唯一有一点点遗憾的是无法做到免费，因为所有保安服务都是有成本的，是需要收费的。所幸的是，云服务大大降低了成本，使得云 WAF 服务成为了大家买得起的网站安全防护服务。同时，我们的创新解决方案得到了阿里云 WAF 的大力支持，特为我公司定制了一个用户能承担得起的包年收费方案，进一步降低了用户使用云 WAF 的成本。

而更加意外和令人兴奋的是，云 SSL 加云 WAF 的方案彻底解决了困惑笔者多年的一个技

术难题—虚拟主机用户无法安装独立的 SSL 证书，而本方案根本就不需要在用户服务器上安装 SSL 证书，用户的网站只需通过 CNAME 域名解析变成 WAF 的源站即可，一个非常巧妙的方案帮助所有虚拟主机网站用户彻底摘掉了“不安全”的帽子，从此以后就再也不用对浏览器显示网站为“不安全”而发愁了。

也就是说，用户可以选择 ACME 解决方案，但只能保证网站有 https 加密，并且自己必须有服务器，必须在服务器上安装 ACME 客户端软件。现在，用户有了新的选择，选择我们的解决方案，则既能保证网站有 https 加密又能防护网站被攻击，而且还不需要动服务器任何地方，不需要安装 SSL 证书，不需要安装 ACME 客户端软件，也不需要自己有服务器，可以是虚拟主机，原网站原封不动，只需做两次 CNAME 域名解析，10 分钟就可以消除所有浏览器的显示“不安全”警告，同时即刻开启防攻击保护，而且这个安全防护是由业界领先的阿里云 WAF 提供。当然，用户的网站是在阿里云还是不在阿里云都没有关系，只要是互联网能访问的网站，都能使用我们的云服务来保障网站安全，这绝对是一个两全其美的最完美的网站安全解决方案。

笔者在规划这个新方案时同时测试了阿里云 WAF、华为云 WAF、腾讯云 WAF 和京东云 WAF，但最终还是选择了基于阿里云 WAF 开发 SSL 证书自动化部署方案，因为我们认为阿里云 WAF 性能、功能和接口更容易集成我们的云 SSL 服务。我们也计划测试微软云 WAF 和亚马逊云 WAF，但是这两家的云 WAF 设置太复杂，非一般人能搞定，所以放弃了测试。就这一点，笔者不得不夸一下我们的国产云 WAF 服务，全部都是傻瓜式一键搞定，很对我们的“一键搞定 SSL”的胃口。所以，我已经计划后续会对接多家国产云 WAF 服务提供商，让我们的用户有更多的选择，满足用户的各种不同的应用需求和适应更多的在云环境。

ACME vs CWAF，你 get 到了？这是”HTTPS” vs “HTTPS+WAF”！”Web 安全 1.0” vs “Web 安全 2.0”！

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。