

## 网站零信任安全三步曲之第二步：云 WAF 防护

零信任是一种安全理念，同样非常适用于网站安全。网站零信任安全的核心之一就是信任每一次 Web 连接，始终验证，放行正常连接和拦截恶意连接。熟悉 WAF 的读者一看这个功能就知道这是 Web 应用防火墙(WAF)的工作，这就是对网络流量的零信任，本文就详细讲解云 WAF 防护。

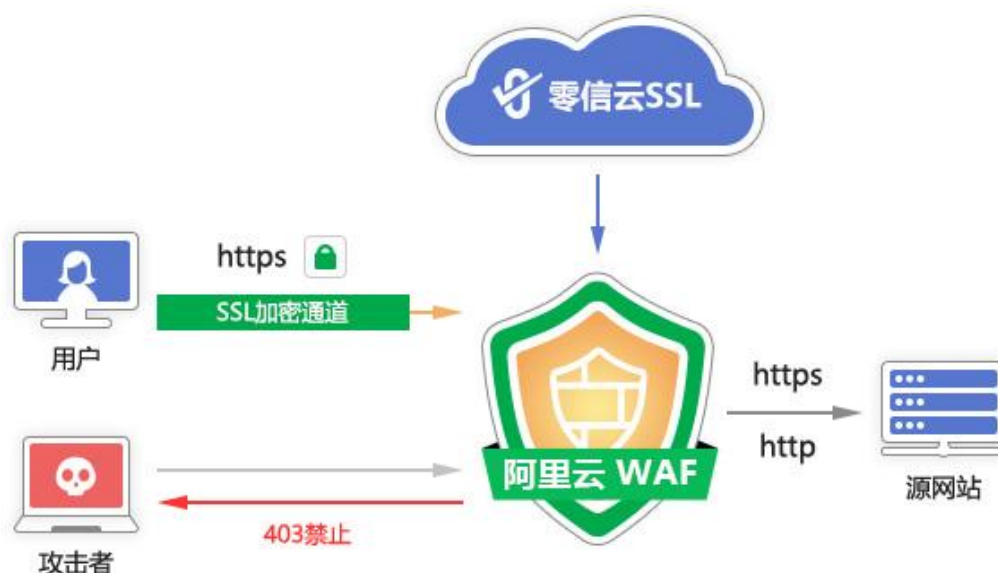
笔者在另一篇博文《[网站零信任安全三步曲第一步：HTTPS 加密](#)》中详细讲解了如何实现网站零信任安全三步曲的第一步的 HTTPS 加密，这是网站安全的基础。但是，网站仅有 HTTPS 加密还是不够的。根据国家互联网应急中心 (CNCERT)发布的 2020 年《中国互联网网络安全报告》数据，2020 年 CNCERT 共监测到我国境内 **53,171** 个(5 万多)网站被植入后门，其中政府网站有 256 个；2020 年，我国境内被篡改的网站数量为 **100,484** 个(10 万多)，其中政府网站有 494 个。2020 年，利用木马或僵尸程序控制服务器对主机进行控制的事件中，控制服务器 IP 地址总数为 **65,865** 个(6 万多)，这些服务器不仅服务器中的数据会被窃取，而且都可以被利用来发起各种攻击。为何发生这么多网站被攻击事件，当然是因为网站没有安全防护。

所以，网站安全不仅需要 HTTPS 加密，还需要云 WAF 防护，两者都是不可或缺的。云 WAF 防护能有效防止各种网络攻击，防止信息从浏览器到达服务器后的被非法窃取和非法篡改。HTTPS 加密保障机密信息安全到达服务器，而信息到达服务器后防止各种网络攻击的工作就只能由 Web 应用防火墙来完成了，没有 WAF 防护，HTTPS 加密也就是失去了意义了！这一点非常重要。HTTPS 加密和 WAF 防护各司其职、各管一段！

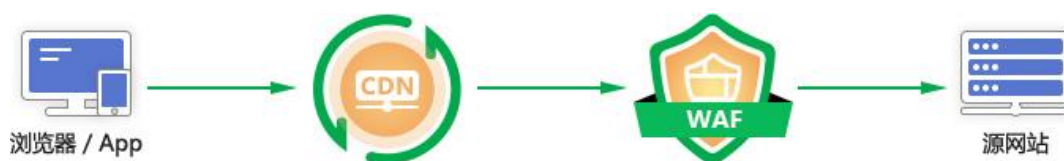


既然网站安全需要云 WAF 防护，也需要 HTTPS 加密，那如果有一个技术能一箭双雕同时实现 HTTPS 加密和云 WAF 防护，那岂不是非常美哉？！零信网站安全云服务就是这样的一个完美解决方案，一个对 Web 流量的零信任安全解决方案，由云 WAF 检查每一次 Web 连接，放行正常连接和拦截恶意连接。用户只需按要求做一次 CNAME 解析就可以自动完成域名

验证，零信云 SSL 服务自动为网站签发所需的 SSL 证书并自动配置到云 WAF 上使用，只需再做一次 CNAME 域名解析即可启用云 WAF+HTTPS 加密服务。这是一个基于阿里云 WAF 服务和自研云 SSL 服务打造，完美快速全自动实现 HTTPS 加密和云 WAF 防护，完美满足“入侵防范”、“恶意代码防范”、“数据完整性(防篡改)”、“通信传输”、“数据保密性”等五个方面的等保合规要求。



而为了提高网站响应速度和提升用户体验，推荐用户采用 CDN+WAF 架构，有两种实现方式，方式一如下图所示，用户端流量先到 CDN，由 CDN 转发到 WAF，WAF 清洗流量后再到源站 Web 服务器，实现网站加速、流量检测和攻击拦截。



这种方式的好处是 CDN 服务提供商和 WAF 服务提供商可以不是同一家服务提供商，都通过 CNAME 方式接入。但是，这种方式需要把各种流量包括恶意流量都集中到中心 WAF 中，不仅浪费了流量而且无法做到就近快速响应。笔者推荐采用 CDN+边缘 WAF 方式，如下图所示，在流量的接入边缘拦截恶意流量，只让正常流量通过 CDN 网络转发，不仅节省流量带宽，而且能提升正常流量的转发速度，无需把所有流量都转发到中心 WAF 来处理。



零信网站安全云服务就是采用了第二种方式，实现了本地流量的快速清洗和把源站数据快速转发给本地用户，直接在“最后一公里”解决安全防护问题，而不是必须到中心云 WAF 来实现安全防护，将大大提高网站的响应速度和提升用户体验。



网站实现了云 WAF 防护，但是网站访问者并不了解，所以，零信浏览器创新地在地址栏直接显示云 WAF 防护标识，让网站访问者对网站的安全防护状况和是否“等保合规”一目了然，能有效增强网站访问者的在线信任。网站是否有云 WAF 防护，在零信浏览器创新集成的网站安全体检评级中占比 20%，有了云 WAF 防护能有效提升网站安全评级级别。



总之，为了网站安全，必须对每一次 Web 连接零信任，必须检测每次连接是否是恶意攻击，并实时阻断攻击连接，放行正常连接，这就要求网站必须有云 WAF 防护。零信网站安全

云服务不仅让用户全自动实现了云 WAF 防护，实现了网站零信任安全三步曲的第二步，而且让用户可以使用零信浏览器实时了解这一步的实际实施结果，以简单明了的方式对比了解使用零信网站安全云服务之前后的网站安全状态的提升情况(安全评级级别会上升)，让用户对自己的网站安全状况放心，以便可以专注于做好自己的业务。

**王高华**

2022 年 6 月 22 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。

