第 11 讲 什么是 CDN/WAF？什么是国密 CDN/WAF？

CDN 是英文 Content Delivery Network 的缩写，中文名称：内容分发网络，通过在网络各处放置节点服务器所构成的在现有的互联网基础之上的一层智能虚拟网络，CDN 系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上。其目的是使用户可就近取得所需内容，改善网络拥挤的状况，提高用户访问网站的响应速度。CDN 已经成为各大云服务提供商的标配服务产品之一，并且由于竞争激烈，而使得 CDN 的费用已经大幅降低到所有网站都能承受的水平。

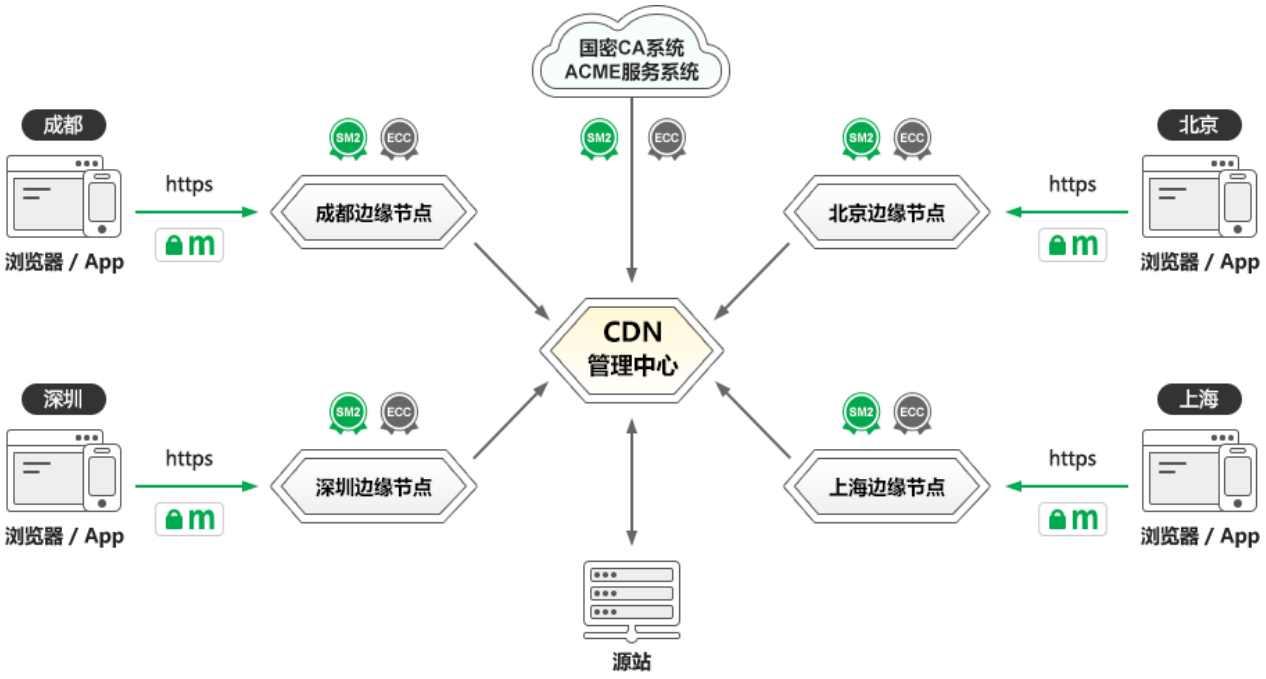
WAF 是英文 Web Application Firewall 的缩写，中文名称：Web 应用防火墙，是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。可以是用户本地化部署的硬件产品，也可以是一个云服务。由于针对各种 Web 应用的攻击如：SQL 注入、跨站攻击、网站挂马等等已经成为普及的趋势，所以，不仅各种安全厂商纷纷推出各种硬件 WAF 产品，而且各大云服务提供商也纷纷提供云 WAF 服务，并且已经成为了各大云服务提供商的标配服务产品之一。

读者也许会有疑问：密码讲堂怎么讲起这些网络服务产品和网络安全产品了，是否跑题了？还真的没有，所有网络服务和网络安全产品都离不开密码。这就是为何笔者在 CDN 和 WAF 之前加了两个字“国密”。传统的 CDN 和 WAF 产品将会在谷歌的“90 天证书革命”中发挥新的重要作用，迸发新的活力，国密 CDN 和国密 WAF 将为各大 CDN/WAF 服务提供商和 WAF 硬件厂商带来更多的市场机会和提升产品核心竞争力。

早期的 CDN 是只能分发 http 明文传输流量的，但是由于 https 加密已经成为了必须，所有浏览器都对明文 http 流量显示为“不安全”，这使得 CDN 服务在最近几年几乎都已经支持 https 加密，不支持 https 加密的 CDN 应该已经没有市场了，因为用户网站需要 https 加密。这个支持 https 加密是需要用户在选购了 CDN 服务后自己再去向 CA 申请 SSL 证书，把 SSL 证书的私钥和公钥证书都手动上传到 CDN 系统后台启用 https 加密功能，这个过程同用户自己申请 SSL 证书部署到网站是一样的痛苦！现在的 SSL 证书有效期是 1 年，也就是说一年痛苦一次。但是，如果 SSL 证书有效期变成了 90 天怎么办？仍然要求用户每 90 天申请和上传 SSL 证书，也就是说一年会痛苦四次！这不是用户能接受的方案，这就是需要 CDN 支持自动化配置和续期 SSL 证书。而对于正在增长的国密 https 加密的应用需求，则需要 CDN 同时支持国密算法和国密 SSL 证书，当然，也一样必须支持自动化配置国密 SSL 证书。

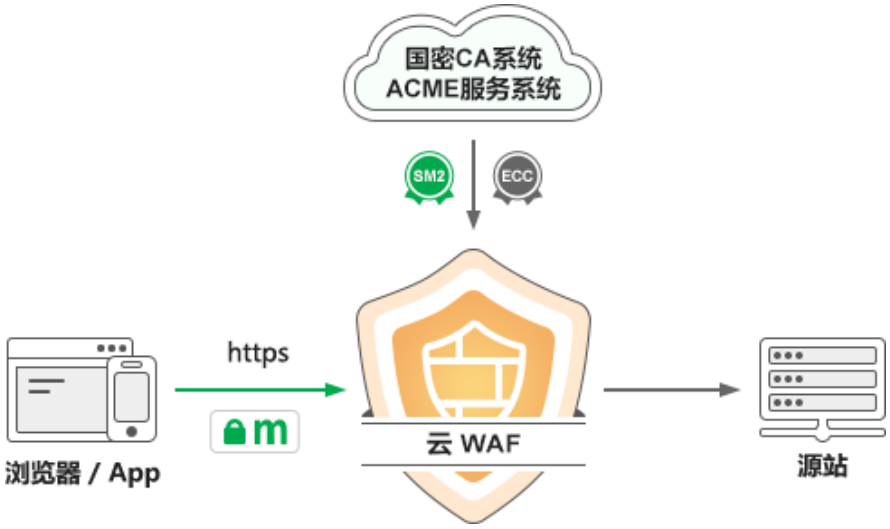
用户需要自动化配置国际 SSL 证书和国密 SSL 证书的这个应用需求，给了 CDN 服务提供商一个新的市场机会，新型 CDN 服务必须是能自动化为用户配置双算法双 SSL 证书的云服务，而不是让用户自己先向 CA 申请 SSL 证书，再手动上传 SSL 证书到 CDN 系统！新型 CDN 服务必须是支持国密算法和国密 SSL 证书的云服务，同时支持自动化配置国际 SSL 证书和国密 SSL 证书，双证书自动化部署和自动化续期，满足用户国密合规和全球信任的 https 加密应用需求。也就是说，CDN 服务不再只是一个内容分发网络服务，而且还是一个让用户零改造实现国密 https 加密的创新服务。

如何才能实现这个创新功能？当然是 CDN 系统需要改造支持国密 ACME 协议、支持国密算法和国密 SSL 证书，对接国密 ACME 系统，自动化为用户的网站域名配置双算法 SSL 证书，实现 https 加密。而用户网站作为 CDN 源站则是零改造，只需做 CNAME 域名解析即可。CDN 服务不仅为用户提供了高速内容分发服务，而且为用户提供零改造实现国密 https 加密服务，实现了自动化为用户配置双算法 SSL 证书，让用户无需向 CA 申请双 SSL 证书，无需担心 SSL 证书过期，这就大大减少网管工程师的工作负担，让工程师可以专心做好自己的其他更重要的业务。同时，这也大大提升了 CDN 服务的核心竞争力！



同理，对于 WAF 设备厂商和云 WAF 服务提供商，也不能仅仅提供 WAF 服务，仅仅提供 http 明文传输 WAF 防护，应该支持 https 加密，自适应加密算法同时支持国际算法和国密算法。但不应该让用户自己去向 CA 申请 SSL 证书，自己配置到 WAF 设备或云 WAF 服务中去

使用 SSL 证书，而应该自动化为用户网站配置双算法双 SSL 证书，实现自适应加密算法的 https 加密。WAF 设备或云 WAF 服务不仅为用户提供了 WAF 防护服务，而且为用户提供零改造实现国密 https 加密服务，实现了自动化为用户配置双算法 SSL 证书，让用户无需向 CA 申请双 SSL 证书，无需担心 SSL 证书过期，这就大大减少网管工程师的工作负担，让工程师可以专心做好自己的其他更重要的业务。同时，这也大大提升了 WAF 设备和云 WAF 服务的核心竞争力！



最后总结一下，传统的 CDN 服务、云 WAF 服务和 WAF 设备，在普及国密 https 加密的大趋势下，必须升级脱变为支持国密算法自动化实现国密 https 加密的国密改造利器，只要我国的所有 CDN 服务提供商、云 WAF 服务提供商、WAF 设备厂商都能支持国密 ACME 标准实现自动化为 CDN/WAF 服务配置双算法双 SSL 证书，为用户提供自动化国密 https 加密服务，则我国普及国密 https 加密就不再是难事了。所以，笔者在本讲为下一代 CDN 服务和 WAF 服务命名为国密 CDN 和国密 WAF，真正实现让密码触手可及，让商用密码真正为保障我国互联网安全做出最大的贡献。

下一讲内容预告 | 第 12 讲 什么是 SSL 加速？什么是 SSL 卸载？什么是 HTTPS 网关？

SSL 证书不是用户所需的产品，用户需要 https 加密！如何实现 https 加密有很多种方案，本讲讲一讲一个硬件网关解决方案，一个让 SSL 加速这个古老的产品重新焕发新活力的解决方案。

王高华

2023 年 5 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。