神奇的 CNAME

CNAME 是英文 Canonical Name (规范名称)的缩写，是域名解析系统中的一种资源记录，用于将一个域名映射到另一个域名，笔者更愿意翻译为“别名解析”。零信网站安全云服务只需用户做两次 CNAME 解析就可以全自动 10 分钟实现 https 加密和云 WAF 防护，用户无需向 CA 申请 SSL 证书，也无需安装 SSL 证书或安装其他客户端软件。本文就给大家讲讲这是如何做到了。

大家都知道，要实现 https 加密必须有 SSL 证书，这是谁也跑不了的事情，但是购买了零信网站安全云服务的用户无需向 CA 申请 SSL 证书，由零信云 SSL 系统自动化帮助用户向 CA 申请证书，而申请 SSL 证书必须完成域名控制权验证，这是国际标准要求的，谁也绕不过去。而如何验证域名控制权？国际标准支持 3 种方式，一是给 webmaster@域名发送验证码，用户在证书申请页面粘贴验证码就可以通过验证。当然还支持其他 4 个邮箱：postmaster@, hostmaster@, admin@, administrator@。这种方式的不方便之处是用户有可能没有这些邮箱，或者即使有这些邮箱，但是无法收到域名验证系统发送的验证码。所以，我们没有采用这种方式来验证域名控制权。还有一种验证方式是要求用户在服务器上的特定目录放置一个特定的内容的文件，这种方式也由于用户可能无法操作服务器而无法实时完成，所以，我们也没有采用这种方式来验证域名控制权。

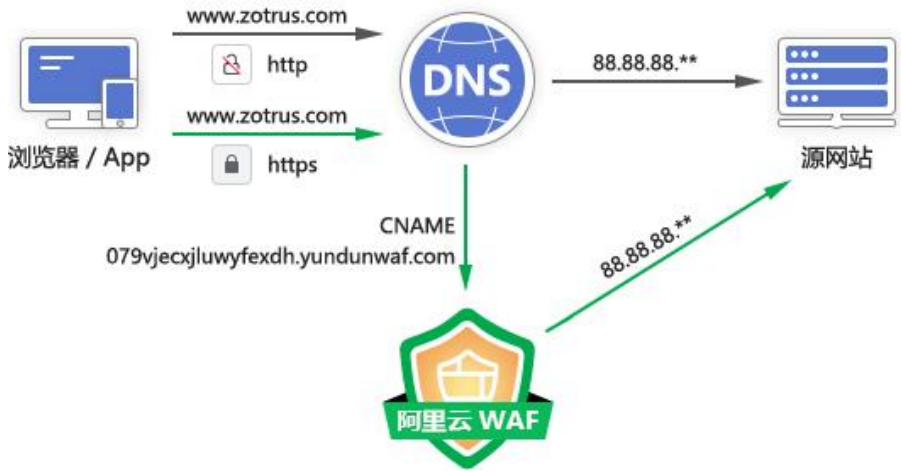
我们采用的是第三种方式-CNAME 验证，由 CA 系统自动生成一个短验证码用于 CNAME 解析的域名，而另一个长验证码用于 CNAME 解析的值，设置完成后提交验证，域名验证系统就会通过域名解析系统获取这两个验证码而完成域名验证。这种验证机制的依据是用户能按要求做域名解析，当然能证明用户拥有此域名的控制权。完成 CNAME 域名验证后就可以自动签发 SSL 证书了。

这是使用零信网站安全云服务必须做的第一次 CNAME 域名解析，证明用户有权使用这个域名，完成验证就可以给这样域名签发绑定此域名的 SSL 证书了。但是，我们并不会把 SSL

证书给用户，用户也并不需要这张 SSL 证书，用户需要的是 https 加密服务。

用户完成域名控制权验证后，系统就会设置云 WAF 服务，并把 SSL 证书部署到云 WAF 上，完成设置后会给用户一个云 WAF 系统的 CNAME 接入网址，用户只需把 www 域名 CNAME 解析到云 WAF 接入网址上即可即刻启用云 WAF 防护和 https 加密服务。

如下图的黑线箭头方向所示，用户在选购零信网站安全云服务之前是 http 明文不安全方式访问网站。如下图绿线箭头方向所示，第 2 次 CNAME 域名解析后，用户访问网站就变成了 https 加密方式访问，先访问云 WAF 服务，由云 WAF 检查是否是合法连接后再去源网站获取用户要访问的资源并返回给用户。CNAME 域名解析重定向了访问路由，不是直接访问网站，而是先访问云 WAF 网址，由云 WAF 负责担任保安职能拦截恶意攻击和放行正常访问，从而保护了网站的安全。



读者应该从上图可以看出，是 CNAME 解析改变了用户访问网站的路由，达到了自动为网站提供安全防护的目的。打一个形象的比喻，原先网站访问者是从一个不安全的没有保安防守的大门(80 端口)进入网站的，现在有了零信网站安全云服务，原先的不安全的大门(80 端口)已经关闭，网站访问者被引导到有保安的另一个大门(443 端口)，不仅检查访问者是否是恶意攻击者并拦截攻击者，而且给正常访问者提供一个加密通道(https)访问网站资源。

这个双防护功能只需两次 CNAME 域名解析就能搞定，CNAME 域名解析起到关键的作用，让用户无需向 CA 申请 SSL 证书，无需安装 SSL 证书或安装任何客户端软件，就可以全自动实现 https 加密和 WAF 防护。所以，笔者才称赞 CNAME 为“神奇的 CNAME”。

王高华

2022 年 6 月 6 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。