第 12 讲 什么是 SSL 加速？什么是 SSL 卸载？什么是 HTTPS 网关？

前几讲讲的内容都与 SSL 证书有关，但笔者明确地告诉读者朋友，用户需要的不是 SSL 证书，需要的是用 SSL 证书实现的 https 加密，用户需要自动化实现 https 加密。如何实现自动化，国际上的解决方案是 Let's Encrypt 提出的解决方案—用户在服务器上安装 ACME 客户端软件，让客户端软件来自动向 CA 系统申请证书并部署 SSL 证书，自动化实现 https 加密。但是，这个方案仅适用于自动化部署国际 SSL 证书，这个方案的缺陷是需要在服务器安装一个软件，这对于很多用户也是做不到，一是不敢动正在运行的服务器，而是不愿意在服务器上安装第三方软件。怎么办？本讲解一个无需安装任何软件的硬件解决方案。

什么是 SSL 加速？英文是 SSL Acceleration, 是指由 SSL 加速卡(SSL Accelerator)来提供 SSL 协议握手消息的加密和解密。SSL 卸载的英文是 SSL Offloading，是指由 SSL 卸载卡来提供 SSL 加密流量解密为明文流量给 Web 服务器处理。前者是针对客户端浏览器来讲的，能加速响应客户端的 https 握手连接；后者则是针对 Web 服务器来讲的，能减轻 Web 服务器的解密负担。

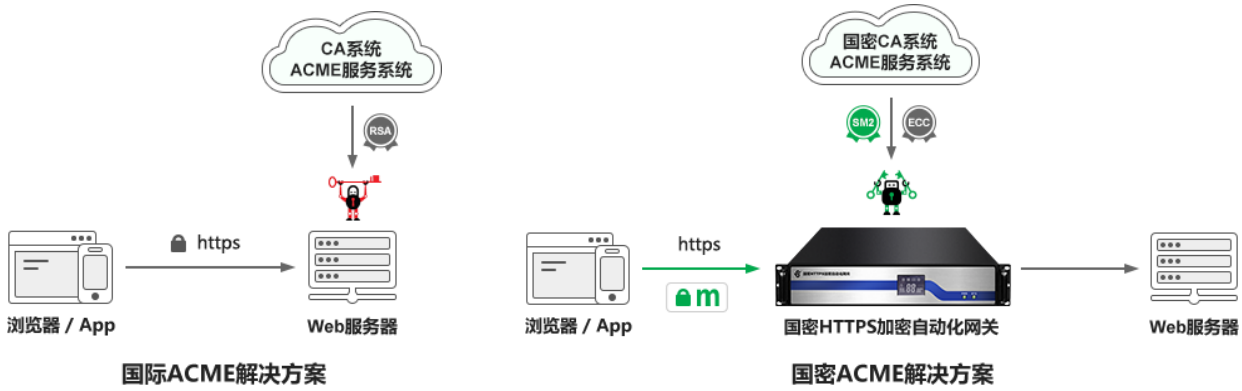
SSL 加速卡和 SSL 卸载卡一般都是同一张硬件密码卡同时提供 SSL 加速和 SSL 卸载功能，这个产品也是一个比较"古老"的产品，从 1994 年有了 SSL 证书实现 https 加密服务后的不久就有了 SSL 加速和卸载卡，因为当时的 Web 服务器性能比较差，SSL 加密和解密几乎消耗了服务器的 30%-60%的资源，所以，必须有一个独立的硬件卡来负责 https 加解密工作，从而减轻服务器的负担。但是，随着 Intel CPU 在 2008 年内置了支持 AES 算法提供加解密功能，以及 CPU 的运算能力的不断提升，https 加密给服务器增加的负担大幅下降到 3%左右，特别是 ECC 算法 SSL 证书的广泛部署使用。这些就使得原先市场上大量的 SSL 加速卡好像突然就消失了，现在能搜索到的厂家已经非常少了，基于 SSL 加速卡实现的 SSL 网关产品也就在市场上很少见了。

既然 SSL 加速、SSL 卸载和 SSL 网关等产品已经在市场上几乎被遗忘了，为何笔者还要在密码讲堂来专门讲这个主题呢？因为笔者看到了这个几乎要被淘汰的产品可以在我国的国密改造中发挥大作用！SSL 网关或称 HTTPS 网关这个比较古老的产品如果结合先进的云密码服务、高性能密码卡和强大的 CPU 处理能力将能派上大用场。

大家都知道国密 https 加密改造很难，要普及国密 https 加密必须是自动化实现，而不是手动改造 Web 服务器和手动部署国密 SSL 证书！国际上的方案是在服务器安装一个客户端软件，

但是这个解决方案也很难用于实现国密 https 加密自动化，因为要实现国密 https 加密必须是 Web 服务器软件也支持国密算法，这就必须改造 Web 服务器软件，但这并不是一件容易的事情，更何况用户的需求是尽量不要动现有的服务器就能实现国密 https 加密！怎么办？

采用 SSL 加速卡实现的 SSL 网关就可以排上大用场了！当然不是传统的 SSL 网关，还需要改造成 HTTPS 加密自动化网关，才能担起自动化实现国密 HTTPS 加密的重任。



国际 ACME 解决方案是在 Web 服务器上安装 ACME 客户端软件，由 ACME 客户端软件自动连接 ACME 服务系统实现自动化签发 RSA 算法 SSL 证书。而国密 ACME 解决方案则无需在 Web 服务器上安装任何 ACME 客户端软件，Web 服务器无需改造支持国密算法，只需在 Web 服务器前部署国密 HTTPS 加密自动化网关，网关已经内置了国密 ACME 客户端软件，会自动连接国密 ACME 服务系统实现自动化签发 SM2 算法 SSL 证书和 ECC 算法 SSL 证书，自动化实现双算法双 SSL 证书部署，自适应加密算法实现 https 加密，自动卸载 https 加密流量并转发到后面的 Web 服务器，实现零改造国密 https 加密。

国密 HTTPS 加密自动化网关就是一个在传统的 SSL 网关的基础上增加了 ACME 功能的零改造实现国密 https 加密改造的创新产品，这是一个让“古老”的 SSL 加密卡在国密改造浪潮中焕发新活力的新物种，能大大降低我国普及国密 https 加密的实施门槛，从而大大加速国密 https 加密在我国的普及应用，大大加快采用国密算法和国密产品来保障我国互联网安全的步伐，大大加快提升我国互联网安全的保障水平。

下一讲内容预告 | 第 13 讲 SSL 证书及相关国际标准

本讲详细讲解 SSL 证书中最重要的 9 个字段的含义和作用，这些字段都是 SSL 证书必须有的而且不能错的字段。可供 SSL 证书使用者、CA 机构和 CA 系统提供商学习参考。

王高华

2023 年 5 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