“国密”无需“改造”，只需部署国密 HTTPS 加密自动化网关

笔者这段时间同多个省市级政务云平台主管有交流，大家都很清楚国密合规的重要和紧迫，但是谈起国密改造，大家都说压力很大，不好改，最关键的一点是不能影响现有政务系统的正常可靠运行，各个局委办的网站都在政务云平台统一管理，有成千上万个政务网站在正常运行，动任何一台物理服务器就可能把某个关键系统给影响了，那就是大事故！绝对不能出事，这一点是第一重要的事情。把现在的 http 网站升级为 https 加密和国密 https 加密变成了次要的事情。但是，又必须做，这就很纠结，很矛盾。

笔者现在是真的非常能理解为何许多政务网站还没有部署 SSL 证书的“不安全”状态了，不是不知道不安全，所有浏览器都会提示“不安全”。也不是经费问题，到处都有免费 SSL 证书可以申请。核心问题是部署 SSL 证书实现 https 加密太难了，更别提实现国密 https 加密！实施 https 改造的前提是不能影响现有业务系统的正常运行！笔者试图推荐他们使用无需改造的网站安全云服务，但是有些主管也不接受这个解决方案，他们不希望政务系统的安全可靠依赖外部的云服务，不管这个云服务提供商有多牛！

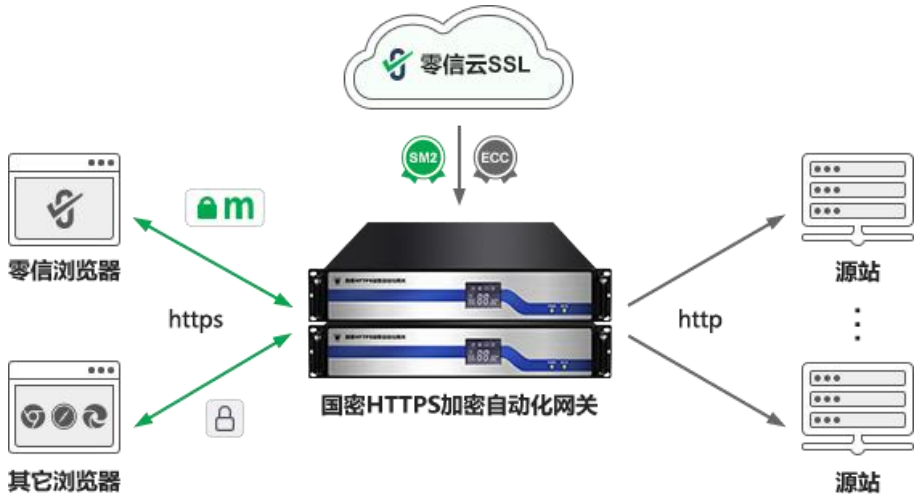
这些主管们提出了一个共同的愿望是：如果现有 Web 系统不用动，也不用自己费力去申请和部署 SSL 证书，能无缝地、业务不停顿的从 http 切换到 https 或者国密 https 加密，但不是外部的云服务，这样的方案则还是可以考虑实施的。

笔者在得到这个来自用户的真实需求后就开始想解决方案了，那不就是需要把零信网站安全云服务本地化部署吗？这个有点难度，因为这涉及到太多的系统了，投资也有点大。是否有更简单的方案？笔者想起了 SSL 卸载卡、SSL 加速卡，这些产品笔者在十几年前就已经接触到了，当时只有国外密码厂商和网络产品厂商做这些产品，现在国内也有厂商做这些产品，并且已经支持了国密算法和国密 SSL 证书。但是，笔者以前一直并不看好此类产品，认为要实现 https 加密只需在 Web 服务器配置一张 SSL 证书即可，并不需要这类产品。虽然这类产品的厂商宣传这类产品能大大减轻 Web 服务器的密码计算负担，但是笔者也看到过国外的研究成果证明现在的服务器硬件对于网站从 http 升级到 https 只增加了服务器的 3%的硬件开销，其增加的开销比加载视频流媒体的开销还要小。

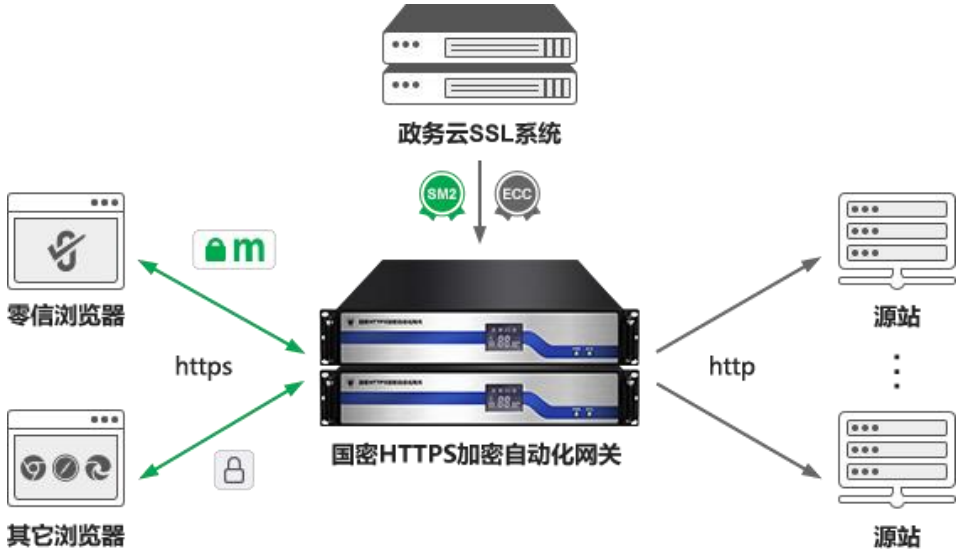
现在，政务云平台主管们提出的实际应用需求让我改变了对 SSL 卸载卡、安全网关之类的产品的作用的看法，这些产品的最大优势是不用改动现有 Web 服务器，可以零改造实现 https 加密，而不是其他功能，可以零改造实现国密 https 加密是关键卖点！当然，前提条件是支持

国密 ACME，能实现自动化为这些产品配置双 SSL 证书，让用户不用操心去申请 SSL 证书和部署 SSL 证书，当然也必须支持国密算法和国密 SSL 证书。有了这个思路，笔者就轻松找到了合作厂商，帮助厂商集成国密 ACME 客户端，并对接零信国密 ACME 服务系统，自动化申请双算法双 SSL 证书，自动化部署双 SSL 证书支持自适应加密算法实现 https 加密、https 卸载转发，这就是今天上线的硬件产品—零信国密 HTTPS 网关。

零信国密 HTTPS 网关是一个集 https 加密响应、https 卸载转发、国密算法模块、SSL 证书自动化、负载均衡等多项功能于一体的高性能网站安全硬件网关设备，这是一个在传统的 SSL 安全网关、SSL 加速卡、SSL 卸载卡等产品的基础上增加了国密 ACME 客户端的能为网关设备自动化配置国密 SSL 证书和国际 SSL 证书实现国密 https 加速和卸载转发的硬件设备，能彻底解决政务系统和大型企业管理系统无法在正在运行的 Web 服务器上部署 SSL 证书或安装 ACME 客户端软件的难题，无需改造原 Web 服务器就可以实现国密 https 加密，满足了用户希望本地化部署系统而不依赖于云服务的自主可控管理应用需求。



有些对安全要求更高的政务云平台，希望能自主签发政务专用 SSL 证书，而不是对接零信云 SSL 平台，则需要把零信云 SSL 系统本地化部署—政务云 SSL 系统(包含国密 ACME 服务系统)，同时定制政务云专用的双算法双 SSL 中级根证书，用于为政务网站自主签发政务专用双算法双 SSL 证书(国密 SSL 证书和国际 SSL 证书)，所有政务系统只信任自己的中级根证书签发的 SSL 证书，能有效保障政务网站免遭 SSL 中间人攻击和假冒 SSL 证书欺诈。国密 HTTPS 网关只需修改为对接政务云 SSL 系统即可，将自动化申请和部署政务云专用的双 SSL 证书，实现更加安全自主可控的国密 HTTPS 加密。



最后总结一下，国密 HTTPS 网关能解决用户难题的核心有两点：一是必须实现国密证书自动化管理，现有网关产品必须改造，内置国密 ACME 客户端，能对接零信国密 ACME 服务系统，能自动化获取国密 SSL 证书和国际 SSL 证书，自动化部署双 SSL 证书实现 https 加密；二是必须支持国密算法和国密 SSL 证书。欢迎更多的相关产品厂商都能提供类似的产品，共同为政务云平台和大型企业私有云平台提供零改造国密 https 加密解决方案，同这些云平台一道努力共同提升我国关键信息基础设施的安全防护水平，共同加速关基系统的国密合规 https 加密普及应用水平。

王高华

2023 年 1 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。