一个网关搞定校园网升级改造诸多难题

暑假正是各个高校升级改造校园网的最佳时机，这就不难理解为何这段时间有多个高校选购了零信国密 HTTPS 加密自动化网关，笔者在这里先公开感谢这些高校网络中心/信息中心领导和老师们对零信产品的信任和支持，特撰文分享这些高校是如何使用零信网关来解决校园网升级改造难题的，以供其他高校在校园网升级改造规划时决策参考，实现多快好省的能真正解决问题的网络升级改造目标。

一、 校园网为何需要升级改造？有哪些需要改造的？

高校校园网经过这么多年的不断建设完善，已经基本上实现了满足高校教学和师生生活的网络需要的建设目标，基本上都实现了一网通行、一网通办和一卡通用等信息化管理。但是，信息化越普及，对信息系统的安全防护要求就越高，校园网急需升级改造的正是网络处处可用而带来的便利的同时带来的网络威胁和数据传输安全威胁，其升级改造核心是 HTTPS 加密和 WAF 防护。

所有教学系统、教学管理系统和师生生活服务系统都需要 HTTPS 加密，否则无法保证这些重要信息系统的大量教学数据和师生数据的机密信息安全，而不仅仅是校园统一身份认证系统的用户名和口令需要 HTTPS 加密保护。一个大学有几十个、几百个管理信息系统，这些系统都需要实现 HTTPS 加密，这就需要向 CA 购买和申请 SSL 证书，需要为每一个网站部署 SSL 证书，这是一个压在网络中心/信息中心主任和老师们头上的一副重担，不仅每上一个业务系统都必须部署 SSL 证书，而且每年统一更新证书时又是一件巨难的工作，这正是难为学校老师了。

不仅如此，随着各种信息系统的普及应用，一切校务和教学都在网上完成，不仅仅是在校园网，而且还需要实现远程教学，基于互联网的全球访问的登录和使用，这些应用使得 WAF(Web 应用防火墙)成为一个必须品，一个校园信息系统必备的应用安全防护产品。而 WAF 系统就是一个 Web 应用反向代理转发服务，必须支持 HTTPS 加密，也就是说，WAF 设备像 Web 服务器一样需要为其部署 SSL 证书，也必须纳入 SSL 证书的安装部署和定期更新工作中。

还有校园网必配的 SSL VPN 网关，原厂默认配置的 SSL 证书是所有浏览器不信任的不安全的自签证书，不仅不方便师生使用，而且存在很多安全问题，必须为其配置全球信任的 SSL 证书，这又给网络中心增加了 SSL 证书的安装部署和定期更新工作。

还有，教育主管部门已经发文要求各高校深入推进 IPv6 规模部署和应用，这就要求高校尽快完成 IPv6 网络升级改造。是否有一个原 Web 服务器不用改造就可以实现支持 IPv6 的 HTTPS 加密访问呢？

还有，校园网 DNS 安全也非常重要，明文 DNS 已经非常不安全，无法保障校园网的各种信息系统的域名解析安全，必须尽快启用最先进的加密 DNS 服务-DNS over HTTPS (DoH)，而 DoH 服务一样需要部署 SSL 证书实现加密 DNS 服务，一样有 SSL 证书的安装部署和定期更新工作。

所有列举的这些与 SSL 证书有关的系统和设备都需要申请和部署 SSL 证书，都需要每年更新一次。而为了保证 SSL 证书密钥安全，国际标准计划把 SSL 证书有效期从目前的 1 年改为 90 天，也即是说，原先一年更新一次的工作量将翻 5 倍，一年要更新 5 次，为上百台服务器和网站系统更新 5 次，这就将是本来就人手紧张的网络中心老师们雪上加霜，使得让所有教学系统都实现 HTTPS 加密成为了不可能实现的目标。

不仅如此，为了保障我国关键信息系统包括高校教务系统安全，国家有关部门已经发文要求各高校全面推进商密改造工作，用商用密码来保障高校教务系统安全，这就要求实现商密 HTTPS 加密，这就需要对原先不支持商密算法的 Web 服务器进行商密改造，以支持商密算法和商密 SSL 证书，这是实现商密 HTTPS 加密所需的改造，只有完成密码算法支持改造后再申请和部署商密 SSL 证书才能实现商密 HTTPS 加密。也就是说，要应用商密算法实现 HTTPS 加密来保障高校教务系统安全，比应用国际算法实现 HTTPS 加密还要难，除了一样有以上困难之外的更多的困难。

二、 是否有解决方案可以实现一箭多雕，搞定所有难题？

笔者在第一部分列出了目前高校校园网要实现所有业务系统和各种网络设备的 HTTPS 加密所遇到的各种问题，这些问题严重影响了高校普及应用 HTTPS 加密来保障教务数据安全和师生个人隐私信息安全。怎么办？是否有好的解决方案？

大家可能会想到 ACME 技术(自动化证书管理环境)，笔者发现有些高校官网已经启用了 Let’s Encrypt 的自动化部署的国际 SSL 证书实现 HTTPS 加密，这就是一个非常好的解决方案—自动化申请和部署 SSL 证书。这个解决方案需要在 Web 服务器安装一个 ACME 客户端软件，但是并不是所有 Web 服务器可以或者放心地安装第三方软件的，有些重要的服务器是不允许安装其他软件的，而有些较老的服务器也许不支持安装这个客户端软件。还有，这个解决方案只能自动化部署 RSA/ECC 算法 SSL 证书，不能实现商密 SSL 证书的自动化部署，无法

实现商密 HTTPS 加密自动化。还有，市场上各种硬件设备如 SSL VPN 和 WAF 设备都还不支持 ACME 技术，仍然需要人工申请和部署 SSL 证书。

也就是说：高校要想普及应用 HTTPS 加密，需要自动化解决方案。但是，国外的 HTTPS 加密自动化解决方案只能解决部分网站的问题，不能解决所有问题，包括：

(1) 不想安装或无法安装 ACME 客户端软件，但是需要实现 HTTPS 加密自动化；
(2) 不想改造或者无法改造 Web 服务器，但是需要支持商密算法实现商密 HTTPS 加密，实现商密 HTTPS 加密自动化；
(3) 不想手动为 SSL VPN 设备和 WAF 设备部署 SSL 证书，但是希望实现 HTTPS 加密方式的 WAF 防护，希望自动化实现安全可信的 SSL VPN 登录；
(4) 不想升级改造 Web 服务器和内部网络以支持 IPv6，但是可实现用户可使用 IPv6 访问 Web 服务器；
(5) 想启用加密 DNS 服务，但不想采用落后的 DNSSEC 技术，希望采用先进的 DoH 加密 DNS 服务，但是又不想增加手动部署和更新 SSL 证书的工作量。

这些都是摆在高校网络中心主管们面前的现实问题和难题，必须寻找一个好的解决方案彻底解决这些难题。

三、 零信网关，自动化搞定校园网升级改造难题

目前市场上可用的能解决以上难题的解决方案只有**一个**：部署零信国密 HTTPS 加密自动化网关，这是一个为我国 HTTPS 加密自动化量身打造的具有国际先进水平的自动化证书管理产品，是目前唯一一个通过商用密码产品认证的国密 HTTPS 加密自动化网关产品，一个采用高性能密码卡打造的高端高性能网站安全硬件密码设备，是一个集 https 加密加速、https 卸载转发、国密算法模块、SSL 证书自动化、WAF 防护、负载均衡等多项功能于一体的专用于 https 加速和卸载的硬件密码设备，内置专业级高性能硬件密码卡实现高速密码运算和网络包转发，并且对内置操作系统、网络协议、SSL/TLS 协议、ECC 算法和 SM2 算法都进行了专业的深度优化，实现了业界领先的极致性能。

零信国密 HTTPS 加密自动化网关最大的特点和特色是自动化申请 SSL 证书、自动化安装 SSL 证书、自动化实现商密 HTTPS 加密，自适应加密算法，支持商密算法和商密证书透明的浏览器采用 SM2 算法实现商密 HTTPS 加密，不支持商密算法和商密证书透明的浏览器采用 ECC 算法实现 HTTPS 加密。这是一个端云一体的创新解决方案，国密 HTTPS 加密自动化网关内置国密 ACME 客户端，自动对接零信云 SSL 系统，自动化完成双 SSL 证书申请、部署和

续期，确保业务系统零改造实现 HTTPS 加密，不间断地自动化为多达 255 个不同域名的业务系统提供自动化 HTTPS 加密服务和 WAF 防护服务。

部署零信国密 HTTPS 加密自动化网关后，可以实现：

(1) **HTTPS 加密自动化**：原 Web 服务器零改造，零安装任何软件，零安装 SSL 证书，5 年内自动化免费为多达 255 个网站申请和部署双算法 SSL 证书(国际 DV SSL 证书+商密 OV SSL 证书)，自动化自适应加密算法实现 HTTPS 加密，自动化完成商密改造。无需每年申请证书、每年续费和重新部署，不仅大大节省大量的 SSL 证书费用，自动化配置的双算法 SSL 证书价值高达 623 万元，而且彻底把网络中心老师们解放出来，让机器去自动化完成申请和部署 SSL 证书这个费时费力的苦力活，让老师们有精力去做更有价值的教学科研工作。

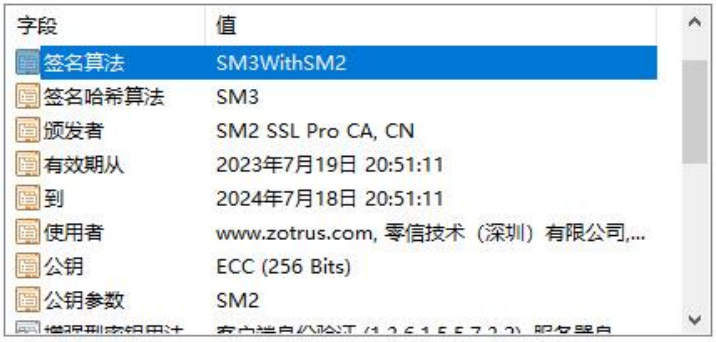
(2) **WAF 防护自动化**：无需再花钱购买 WAF 设备，也无需为部署和更新 WAF 设备所需的 SSL 证书发愁，只需部署零信国密 HTTPS 加密自动化网关，就可以自动化实现 HTTPS 加密方式的 WAF 防护，WAF 防护的检测能力和识别能力都达到 A 级(最高级别)，防护性能甚至超过售价百万的 WAF 设备。

(3) **零改造搞定 IPv6 支持**：原 Web 服务器和内网无需改造支持 IPv6，但用户可以使用 IPv6 访问 Web 网站和业务系统，零信网关实现了 IPv6 到 IPv4 的自动化转换。

(4) **加密 DNS 服务**：只需在零信网关上配置 DoH 服务网站，自动化为其配置双 SSL 证书，实现双算法的 DoH 加密 DNS 服务，支持公网域名和内网域名解析。

不仅如此，某个高校客户网络中心主任告诉笔者，他还有密码学课程教学工作，有了零信网关，就有了真实的教学教具，可以让学生实际体验商用密码算法是什么样的，商密 HTTPS 加密是什么样的，商密 SSL 证书是什么样的，同国际算法 SSL 证书有什么不同，还可以讲商密算法证书透明是什么样的，这些都是以前纸上谈兵讲课所无法到达的更好的教学效果！

这位老师还说：更值得推荐的是零信网关免费配套的国密浏览器—零信浏览器，其为 Windows 打商密算法补丁功能，让讲授 SM2 算法和 SM2 数字证书更容易了，让学生能在电脑上像查看 RSA 算法 SSL 证书一样查看 SM2 算法 SSL 证书，真是太方便了，这个值得超赞。



听到这些话，笔者很是欣慰，很是为零信网关和零信浏览器能为高校的密码学相关课程教学做出了一点点贡献而高兴，这的确不仅是高校客户的意外收益，也是笔者的意外收获。普及商用密码，高校教学是关键，让学生实际体验看得见的商用密码产品和商密 SSL 证书，不仅能吸引青年学子去研究商用密码，提升学习兴趣和学习效率，而且一定能为学子们的将来发展提供了更多的可能和更广阔的空间，因为普及我国的商用密码应用需要更多的密码人才，这是一个利国利民的大事。

有诗为证：

校园网升级改造，密码应用是关键。
部署零信网关，一机搞定所有难题。
自动化，让教师脱身专注教学科研。
真实商密教具，让学习商密更轻松。

王高华

2024 年 7 月 31 日于深圳
