零信®
ZoTrus

校园网升级改造方案

一个网关搞定校园网升级改造诸多难题

https://www.zotrus.com

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。

一、 校园网升级改造遇到了哪些难题?

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。

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?

前面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)，目前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，因为：

01 Web服务器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；

02 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；

03 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；

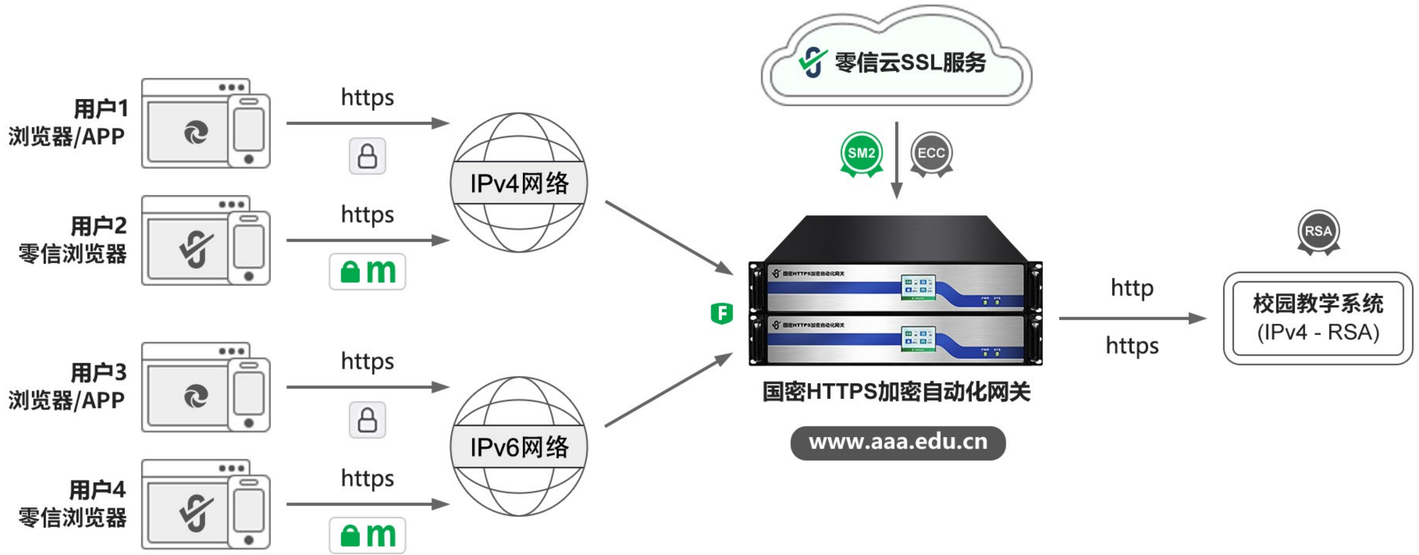
04 不想升级改造Web服务器和内部网络以支持IPv6，但是可实现用户可使用IPv6访问Web服务器；

05 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。

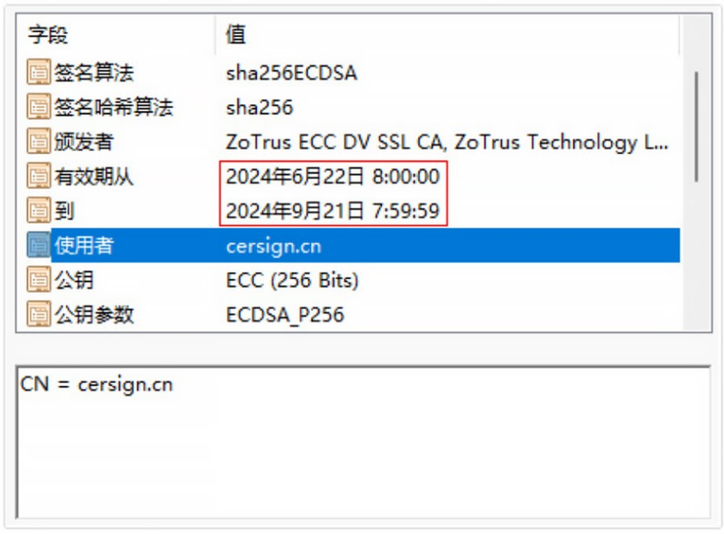
三、 零信网关，自动化搞定校园网升级改造难题

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用户无需想CA申请SSL证书，自动化申请双算法SSL证书、自动化安装双SSL证书，并且已经提前满足将来90天有效期证书政策，自动化实现商密HTTPS加密，自适应加密算法，支持国密算法和国密证书透明的国密浏览器采用SM2算法实现国密HTTPS加密，不支持国密算法和国密证书透明的其他浏览器采用国际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，自动化完成双算法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。

公网SM2 SSL证书



公网ECC SSL证书

部署零信国密HTTPS加密自动化网关后，可以实现：

HTTPS加密自动化

原Web服务器零改造，零安装任何软件，无需去机房生成CSR文件和安装SSL证书，只需部署零信网关，设置网站域名，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，自动化完成国密改造。不用担心证书有效缩短到90天，因为网关会自动化申请证书、自动化续费和重新部署证书，不怕即使将来缩短到1天，不仅大大节省大量的SSL证书费用，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。

国密HTTPS加密自动化

零信网关让原Web系统无需升级改造就可以实现国密HTTPS加密，只需在现有的Web服务器前面部署零信国密HTTPS加密自动化网关即可，自动化配置国密OV SSL证书，自动化实现国密HTTPS加密，原Web系统零改造，自动化完成国密改造，满足各种法律法规的合规要求。更重要的是：这是自动化实现国密HTTPS加密的解决方案，无需向CA购买和申请国密SSL证书和无需人工安装部署，一切工作由机器自动化完成，当然也不用担心SSL证书有效期缩短的问题，反正都是机器自动化定期申请和安装。

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，并且是同时支持国际算法HTTPS加密和国密算法HTTPS加密自动化的WAF防护。

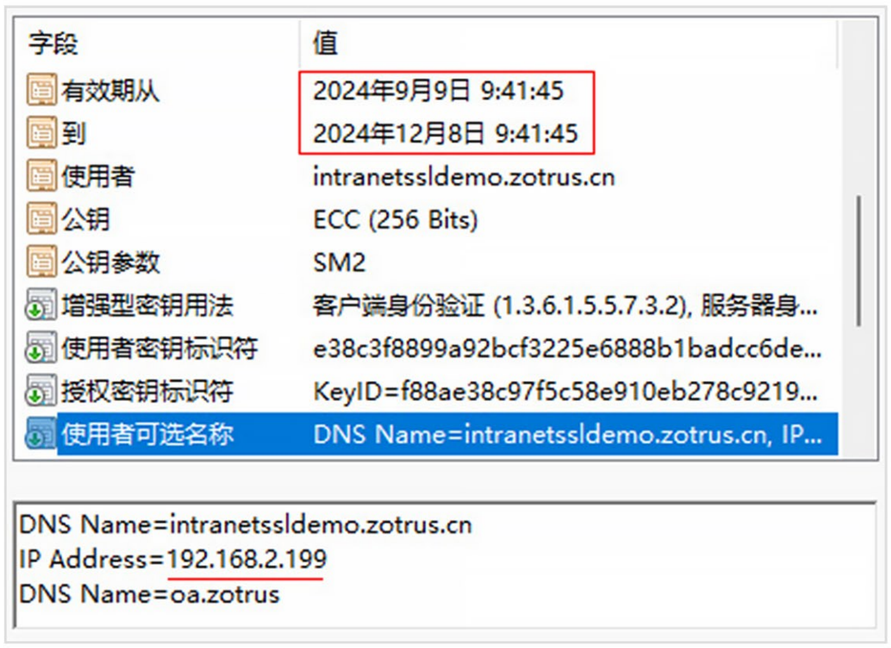
零改造搞定IPv6支持

原Web服务器和内网无需改造，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，并且是HTTPS加密方式的IPv6安全访问。

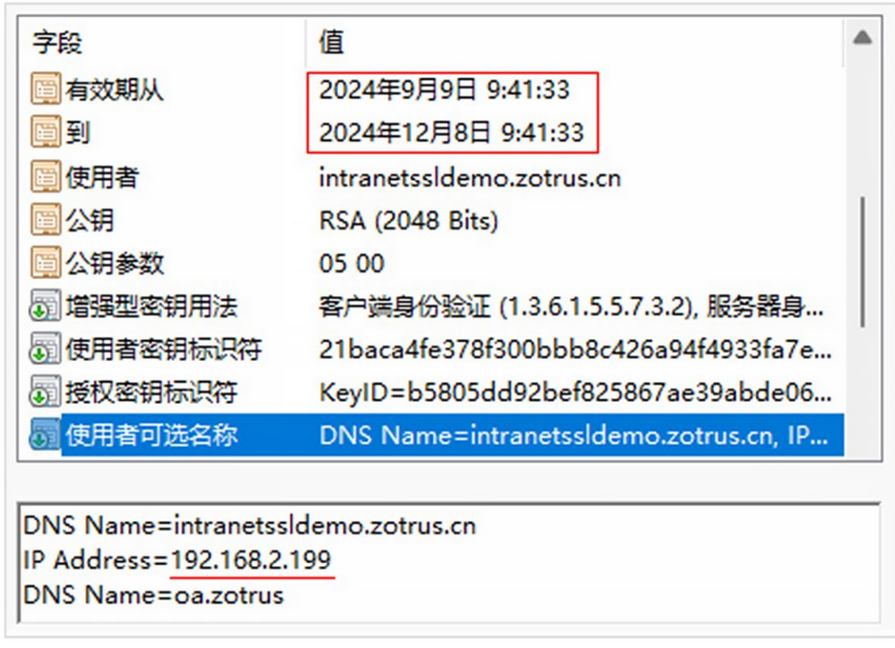
加密DNS服务

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，支持国密算法的浏览器使用国密算法的加密DNS服务，不支持国密算法的浏览器使用国际算法的加密DNS服务，支持公网域名和内网域名解析。

以上解决方案不仅仅适用于位于公网的学校官网、公众服务系统和教务管理系统，同时适用于位于内网的教学科研内部管理系统，零信网关支持自动化申请和部署零信浏览器信任的内网SSL证书(RSA和SM2算法)，支持内网IP地址和内部主机名，以满足学校内网流量加密安全的应用需求。并且支持90天有效期的密钥安全要求，以满足即将到来的国际标准和国密标准要求。



内网SM2 SSL证书



内网RSA SSL证书

四、 零信方案为高校提供四大超值服务

零信技术提供的自动化证书管理方案，可用于高校官网及所有教学管理系统，其超值价值体现在如下4个方面：

01 自动化，彻底解放运维工程师，不再需要人工申请和部署证书，节省人力成本150万元；

02 自动化，配置双算法SSL证书，不再需要花钱买证书，节省证书成本623万元；

03 自动化，WAF防护，不再需要花钱买WAF设备，节省WAF设备购置100万元；

04 免费配套提供干净无广告的基于谷歌内核的高性能国密浏览器，节省国密浏览器购买费用。

上面这些都是看得见的经济效益，还有无法计算的社会效益，主要体现在如下4个方面：

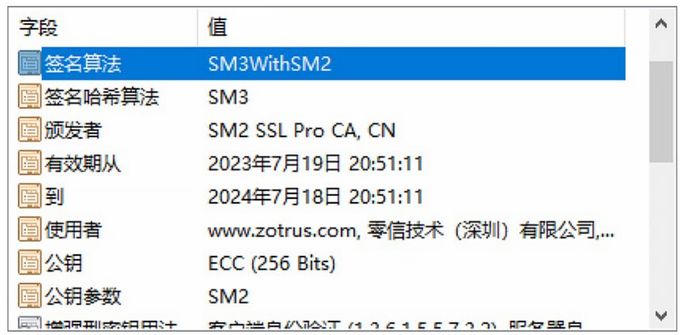
01 自动化，不会出现人工申请SSL证书的忘了到时续期和部署的严重网络安全问题；

02 自动化，实现一站一密钥一证书，彻底解决了人工部署通配证书的共用密钥安全问题；

03 自动化，覆盖校园网所有公网和内网业务系统，实现HTTPS加密全覆盖和普惠安全；

04 自动化，真正实现现有系统零改造，不影响现有业务系统正常运行，无缝升级完成改造。

五、HTTPS加密自动化保障教学科研系统安全，同时为商用密码教学提供了真实可见的教具



校园网有了零信国密HTTPS加密自动化网关，不仅能自动化无忧保障教学科研系统安全，而让高校网络安全课程和密码学课程有了真实的商用密码教学教具，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，教授们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！

而完全免费干净无广告的零信网关配套的国密浏览器—零信浏览器，其为Windows打商密算法补丁功能，让教授们讲授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，非常有利于学生们直观地学习理解商用密码知识。

零信网关和零信浏览器能为高校的网络安全课程和密码学课程教学做出了以上贡献是高校的意外收益，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。