内网更需要 SSL 证书自动化

零信技术一年前上线了证签品牌内网 SSL 证书，由于切实解决了用户急需绑定内网 IP 地址的 SSL 证书的难题，受到了用户的欢迎，已经有很多用户申请使用。今天，零信技术又上线了内网国密 HTTPS 加密自动化网关这个新产品，本文就讲一讲这个历时一年打造的内网网关有什么特别之处，为何需要推出这个内网专用网关产品。

一、 内网流量安全没有得到应有的重视

这里所讲的内网是指不能连接互联网的内部办公网络，如我国的政务外网，各个单位的内部业务管理系统，如医院管理信息系统。笔者曾就医一家深圳三甲医院，其内部管理系统包括护士站的电子白板系统都是明文 HTTP 方式在不安全地运行，谷歌浏览器地址栏非常明显地显示“不安全”，但是没有人关心这个。这非常不安全，不符合《医疗卫生机构网络安全管理办法》中的数据传输加密要求，无法保障机密医疗数据的安全，也严重违反了《数据安全法》对机密数据传输必须采用加密措施的合规要求。

医院管理信息系统只是笔者发现的一个内网流量不安全的案例之一，其实大量的政务和企业办公内网系统也都是明文 HTTP 方式在运行，这些普遍被认为是内网的网络其实已经是一个跨楼层、跨大楼、甚至跨城市的一个大的内联网，这些内网管理信息系统之所以仅限于内网运行，也正是由于这些内网管理的数据非常重要，几乎全部都是需要保护的机密信息。但是，这些机密信息一直在以 HTTP 明文传输方式裸奔，非常不安全，相关单位必须高度重视，必须实现 HTTPS 加密保护。

二、 内网 SSL 证书仍然存在公网 SSL 证书一样的人工安装部署问题

零信技术两年前就充分认识到保护内网流量安全的重要性和紧迫性，历时一年打造了内网 SSL 证书应用生态，推出了零信浏览器信任的证签品牌内网 SSL 证书，受到了广大用户的欢迎。但是，内网 SSL 证书同公网 SSL 证书一样，仍然需要用户在线申请证书、完成域名验证和单位身份认证、在 Web 服务器上安装 SSL 证书，仍然是一个非常繁琐的工作，特别是各种内部管理系统都是在日夜为用户提供服务之中，不能为了安装 SSL 证书而重启 Web 服务，这是一个用户遇到的实实在在的难题。

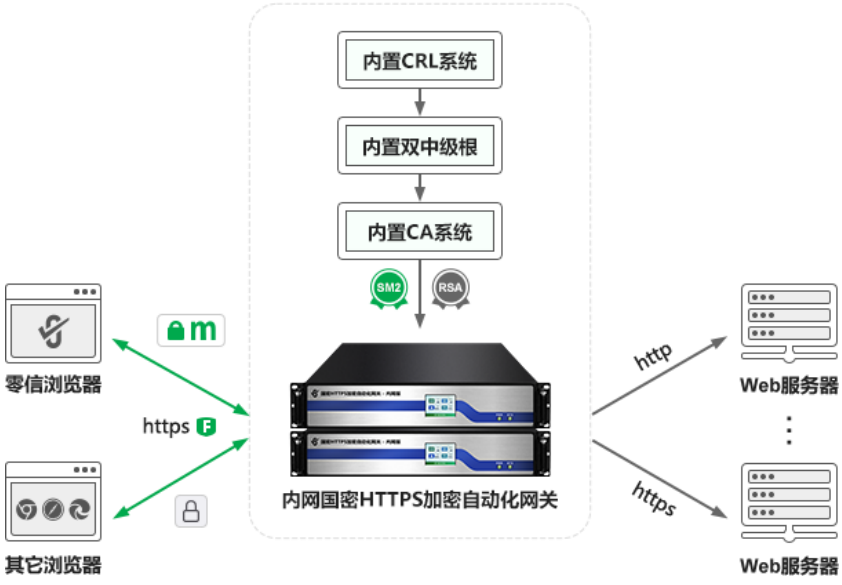
同时，为了满足国密合规和等保合规的要求，内部管理信息系统也需要国密 HTTPS 加密

改造，这就是难上加难，安装 RSA 算法 SSL 证书只需重启一下 Web 服务器，而安装国密 SSL 证书则需要升级改造 Web 服务器，常用的 IIS 服务器软件是无法升级改造支持国密算法的，所以，无论用户安装 RSA 算法内网 SSL 证书还是 SM2 算法内网 SSL 证书，都遇到了不少部署难题。这些难题严重打击了内网系统管理员部署 SSL 证书的积极性，只能是掩耳盗铃地祈祷不会出现机密数据泄露事件了，即使内网用户天天看到浏览器提示“不安全”。

三、 零信内网网关，实现内网 SSL 证书的“自给自足”，彻底解决内网 HTTPS 加密难题

也正是由于充分了解到用户在部署内网 SSL 证书时存在的诸多困难，零信技术在推出内网 SSL 证书后继续寻找更好的解决方案，那就是今天推出的零信国密 HTTPS 加密自动化网关内网版，这是在 2023 年全球首发零信国密 HTTPS 加密自动化网关公网版之后的又一个产品创新，因为内网是不能连接互联网的，那就无法连接零信云 SSL 服务系统，无法实现端云一体的 SSL 证书自动化管理，所以，已经在公网(互联网)广泛部署使用的零信国密 HTTPS 加密自动化网关无法在内网部署使用，虽然公网版网关已经支持为内网 Web 服务器自动化签发内网 SSL 证书，但是前提是网关必须部署在公网上。

要想在内网实现 SSL 证书自动化，唯一可行的解决方案就是由内网网关实现 SSL 证书“自给自足”，自己能给用户内网网站签发浏览器信任的双算法内网 SSL 证书，这就需要把签发 SSL 证书的 CA 系统简化为一个迷你版本，并且必须有签发内网 SSL 证书的中级根证书，还必须有证书吊销管理系统。如下图所示，零信内网网关内置了 CA 系统，用于签发内网 SSL 证书，而签发 SSL 证书的中级根证书密钥则由网关内置的通过商用密码产品认证的密码卡负责生成和管理，并由此密钥来签发双算法内网 SSL 证书。同时，内网网关内置 CRL 系统，用于吊销内网 SSL 证书和浏览器查询证书吊销信息，为内网用户提供公网 SSL 证书一样的证书吊销服务。



零信网关内置 CA 系统签发的双算法 SSL 证书，零信浏览器信任，这是因为内网网关内置的双算法 SSL 中级根证书是由零信浏览器预置信任的 SM2 和 RSA 算法内网专用根证书签发的，仅限于为内网网关用户签发固定单位名称和单位公网域名的双算法内网 SSL 证书。只要内网用户电脑安装了零信浏览器，不仅能正常显示加密锁标识和国密加密标识，实现国密 HTTPS 加密，而且其他常用的浏览器也会信任内网网关自动配置的 RSA 算法内网 SSL 证书，内网用户仍然可以继续使用其常用的仅支持 RSA 算法的浏览器，所有浏览器都不会提示“不安全”，都能安全可靠地实现 HTTPS 加密连接到内网 Web 应用系统。

本次发布的零信内网国密 HTTPS 加密自动化网关支持 3 种不同的 CPU 类型(Intel 和海光)，提供两种不同体型的产品，其中基于英特尔凌动 CPU 的小型内网网关，只有 1.2 公斤，一本书大小，非常适合于中小企业自动化解决内网管理信息系统的 HTTPS 加密难题。而另两款 2U 标准网安设备机箱的内网网关，则能满足政务外网、大中型企事业单位内网的各种应用场景的 HTTPS 加密自动化应用需求，最多支持 510 个内网网站系统，推荐双机热备部署，确保为内部管理系统提供可靠的不间断的 HTTPS 加密自动化和 WAF 防护自动化服务。

四、 只有实现内网 SSL 证书自动化，才能保障内网流量安全

零信内网国密 HTTPS 加密自动化网关采用了同公网 SSL 证书自动化管理(ACME)一样的技术思路，同时解决了内网无法连接云 SSL 证书自动化管理服务系统的难题，做到了双算法内网 SSL 证书的“自给自足”，比公网网关需要依赖 ACME 云端服务更可靠，彻底解决了内网流量明文传输裸奔的技术难题，必将成为解决内网流量安全的首选产品。

内网之所以称之为内网，是因为其流量都是机密数据，比公网更需要 HTTPS 加密。而 HTTPS 加密需要 SSL 证书，内网更需要 SSL 证书自动化，因为内网应用系统不能停止运行来安装 SSL 证书，不能停止运行来完成国密算法支持改造，所以，唯一的完美解决方案只有在 Web 服务器前面部署内网国密 HTTPS 加密自动化网关，实现零改造的从明文 HTTP 无缝升级到 HTTPS 加密，并且是国密 HTTPS 加密，真正用国产密码来保障内网机密数据传输安全，切实保障内网流量安全，满足用户等保和密评合规要求。

王高华

2025 年 3 月 27 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 205 篇(共 59 万 9 千多字)和英文 88 篇(11 万 6 千多单词)。